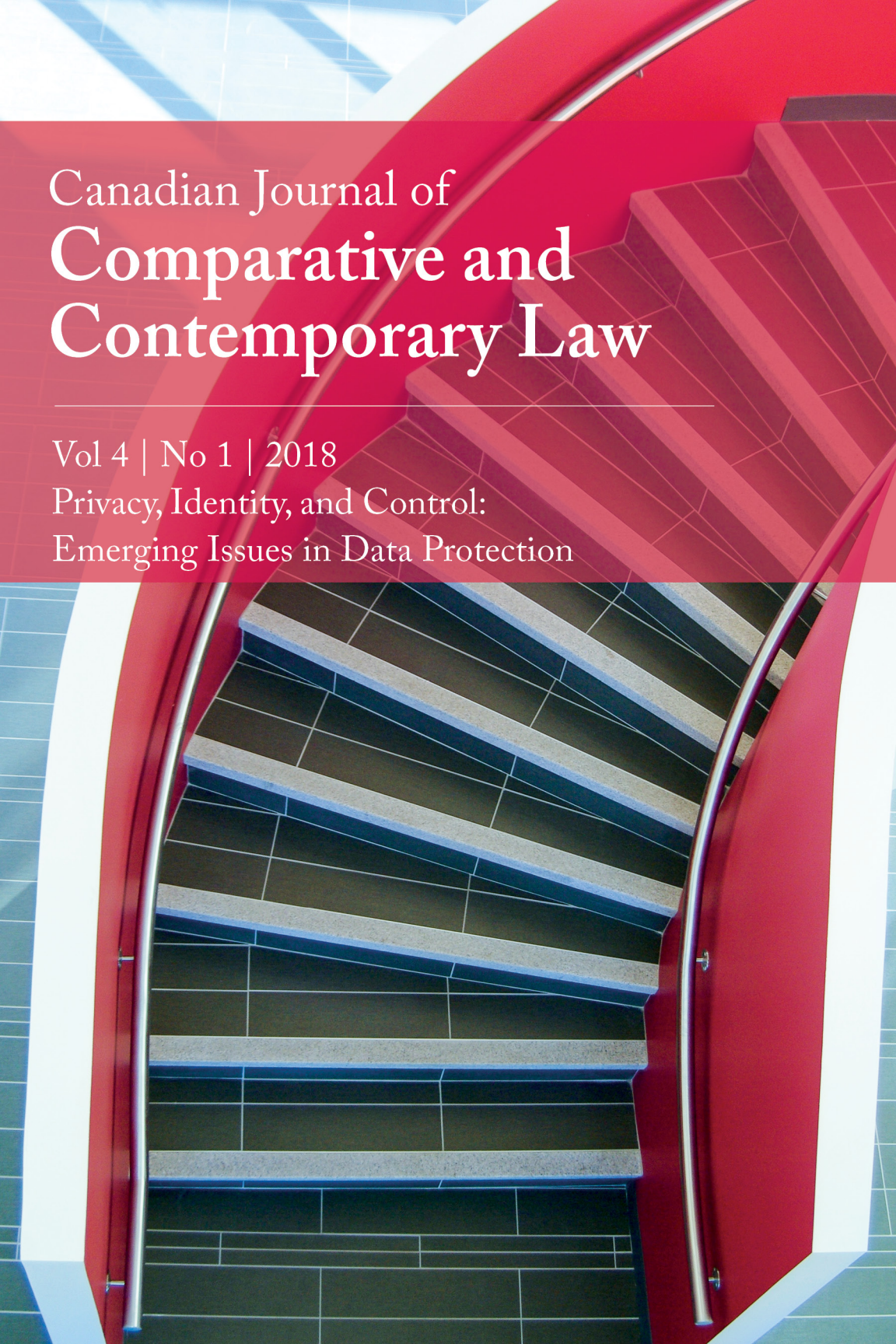

Canadian Journal of Comparative and Contemporary Law

Vol 4 | No 1 | 2018

Privacy, Identity, and Control:
Emerging Issues in Data Protection

Canadian Journal of
Comparative and Contemporary Law

Vol 4 | No 1 | 2018

Privacy, Identity, and Control: Emerging Issues in Data Protection

The CJCCL is published by
The Canadian Association of Comparative and Contemporary Law
at Thompson Rivers University
Kamloops, BC

Canadian Journal of Comparative and Contemporary Law

Publication

The Canadian Journal of Comparative and Contemporary Law (CJCCL) is an open-access publication that is available online at http://www.cjccl.ca. Hardcopies can be ordered on request. Each issue focuses on a particular theme or area of law. The CJCCL encourages contributors to take a comparative approach in their scholarship.

Editorial Policy

All submissions are subject to peer review process.

Submissions

The Journal accepts the following types of manuscripts:

(i) Articles between 8,000 to 15,000 words in length;

(ii) Case Comments between 3,000 to 6,000 words in length; and

(iii) Book Reviews less than 3,000 words in length.
Please visit our website for more details.

Copyright and Open-Access Policy

Contact Information

Canadian Journal of Comparative and Contemporary Law

Thompson Rivers University
Faculty of Law
900 McGill Road
Kamloops, BC, Canada V2C 0C8

E-mail: editor@cjccl.ca
Web: http://www.cjccl.ca

Cover Photo

The front cover depicts the main stairwell that leads to the atrium of Thompson Rivers University, Faculty of Law. The back cover depicts the distinct exterior of the Faculty of Law. The curved design of the roof was inspired by the natural beauty of the mountains visible from the building.

ISSN 2368-4046 (Online)
ISSN 2368-4038 (Print)
ISBN 978-1-9994425-0-7

This Issue should be cited as (2018) 4(1) CJCCL

Canadian Journal of Comparative and Contemporary Law

List of Contributors

Rosalie Silberman Abella, Justice, Supreme Court of Canada.

Jane Bailey, Professor, University of Ottawa Faculty of Law
(Common Law Section).

Fiona Brimblecombe, Tutor in Law and Doctoral Candidate,
Durham Law School.

Jacquelyn Burkell, Associate Professor, University of Western Ontario
Faculty of Information and Media Studies.

Avner Levin, Professor, Law & Business Department,
Ted Rogers School of Management, Ryerson University.

N.A. Moreham, Reader in Law, Victoria University of Wellington.

Moira Paterson, Professor of Law, Monash University, Melbourne.

Gavin Phillipson, Professor of Law, Durham University.

Megan Richardson, Professor of Law and Joint Director,
Centre for Media & Communications Law, The University of Melbourne.

Andrea Slane, Associate Professor in Legal Studies,
University of Ontario Institute of Technology.

Julian Wagner, Lecturer at the Faculty of Law (Chair of Prof Dr Spiecker gen.
Döhmann, LLM), Goethe University, Frankfurt am Main.

Normann Witzleb, Associate Professor at the Faculty of Law,
Monash University, Melbourne.

Canadian Journal of Comparative and Contemporary Law

Volume 4 | number 1 | 2018
Privacy, Identity, and Control:
Emerging Issues in Data Protection

Foreword i
Justice Rosalie Silberman Abella, Supreme Court of Canada

Articles

Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression 1
Fiona Brimblecombe & Gavin Phillipson

Equality at Stake: Connecting the Privacy/Vulnerability Cycle to the Debate about Publicly Accessible Online Court Records 67
Jacquelyn Burkell & Jane Bailey

Privacy by Design by Regulation: The Case Study of Ontario 115
Avner Levin

Abandoning The "High Offensiveness" Privacy Test 161
N.A. Moreham

Regulating Surveillance: Suggestions for a Possible Way Forward 193
Moira Paterson

"A Virtual 'Puppet'": Performance and Privacy in the Digital Age 231
Megan Richardson

Information Brokers, Fairness, and Privacy in Publicly Accessible Information 249
Andrea Slane

When is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws 293
Normann Witzleb & Julian Wagner

Foreword

Justice Rosalie Silberman Abella
Supreme Court of Canada

The Canadian Journal of Comparative and Contemporary Law has produced yet another invaluable intellectual contribution to yet another intellectually dynamic area of law. To tackle the privacy issues in Data Protection is to scrutinize the past in order to make brave predictions about an unknowable future about technology, an overgrown field with a haphazard array of fences in need of repair.

This volume will be an outstanding source of insights for anyone who cares about the relationship between privacy and progress, and its impact on who we are as individuals, as a society, and as a global community. This core mission — assessing the future of privacy in technology's revolutionary wake — gets careful and probing scrutiny in this volume.

Fiona Brimblecombe and Gavin Phillipson explore the implications of the European Union's new "right to be forgotten" found in Article 17 of the General Data Protection Regulation, and how the Strasbourg Court's privacy jurisprudence has adapted to the revised informational contours. The impact of the right to be forgotten is also developed in Jacquelyn Burkell and Jane Bailey's article on how unredacted online public access to court records may have a disproportionately harmful impact on vulnerable groups, raising interesting questions about the role of equality rights.

Ontario's "Privacy by Design" attempts to regulate privacy through the introduction of facial recognition technology in some existing cameras in casinos and the expanded use of cameras in the public transit system, offer a case study by Avner Levin into what works and what works less well. His call for a collaborative regulatory model is echoed throughout the volume. N.A. Moreham compares how different jurisdictions (England, Ontario, and New Zealand) assess privacy interests in the torts context, arguing that New Zealand's test — the "high offensiveness" privacy test — is ultimately ineffective and should be replaced by a test

looking at what "reasonable expectation of privacy" a plaintiff has in the information or activity in question.

A call for greater privacy protection from ubiquitous surveillance practices is the focus of Moira Paterson's review of the tests and assumptions that need to be revisited and strengthened in this context. Megan Richardson moves us towards the internet and the profound risk it poses not only to an individual's privacy, but to the ability to control his or her personal identity, and, relatedly, dignity.

Looking at how the European Union, the United States, and Canada deal with personal information that has become public, leads Andrea Slane to consider what role the concept of fairness should have in dealing with the online marketplace. And Norman Witzleb and Julian Wagner offer a comparative approach to data protection laws in Australia, Canada and the European Union, outlining various approaches to personal information, identity, and privacy.

The dizzying legal and policy options at play in all of these wonderfully thoughtful articles, seem at the same time to suggest urgency and caution. They are a timely and humbling Venn diagram of intersecting problems, solutions, concerns, and aspirations. The implications of the intensity, pervasiveness and speed of technological transformations are compellingly reviewed in the articles by Brimblecombe and Phillipson and by Patterson. The resulting need for more robust and proactive legislative (and judicial) responses are magnetically covered in the article by Paterson, but also in those of Burkell and Bailey, Levin, Slane, Witzleb and Wagner. And finally, the emphatic need for humanity and dignity in the social network universe is powerfully elucidated not only by Slane, Burkell and Bailey, but also by Brimblecombe and Phillipson, Moreham and Richardson.

I feel lucky to have had the chance to learn from these authors, and congratulate them — and the editors — for enriching us with their insights and inspiration.

Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression

Fiona Brimblecombe* & Gavin Phillipson**

This article considers how the newly-formulated "Right to be Forgotten" in Article 17 of the EU's new General Data Protection Regulation *will apply to "online expression", that is, content placed online via social and other forms of media. It starts by seeking to refute the argument that the widespread sharing of personal information online means that digital privacy no longer matters, considering in particular the key role that privacy as informational control plays in self-actualisation and how the advent of a right to erase may alter judicial understandings of informational autonomy. It goes on to consider some of the key interpretive dilemmas posed by Article 17, in particular the questions of when individuals and online intermediaries may be fixed with obligations under the Regulation and who may claim the broad "journalism exemption"; in doing so it contests the notion that the privacy obligations of social media platforms like Facebook should invariably be treated differently from those of search engines like Google. It then goes on to argue that the right to privacy enshrined in Article 8 of the* European Convention on Human Rights, *as interpreted by the Strasbourg Court, is likely to be an important factor in the interpretation of the new right, and how it is balanced with freedom of expression. Using a variety of data dissemination scenarios it considers how Strasbourg's 'reasonable expectation of privacy' test, and the factors that underlie it, might apply to the resolution of different kinds of erasure claims under Article 17. In doing so it analyses the applicability of a number of relevant factors drawn from the Strasbourg case law, including the content of the personal data in question, its form, whether the data subject is a "public figure", implied "waiver" of privacy rights, how the data was collected and disseminated and whether it relates to something that occurred in a physically public location.*

---

* Tutor in Law and Doctoral Candidate, Durham Law School, Durham University.

** Professor of Law, Durham Law School, Durham University. The authors would like to thank David Erdos, Kirsty Hughes and Tom Bennett for comments on all or part of an earlier draft and David Erdos for numerous helpful discussions: the usual disclaimer applies.

I. Introduction
II. Social Media and Self-Disclosure: The Abandonment of Privacy Online?
A. Why the Need for a Right to be Forgotten?
B. Theoretical Dimensions
III. The Right to be Forgotten: Key Interpretative Issues
A. The Focus of This Article
B. Article 17 *GDPR*: The Basics
C. Some Key Interpretive Dilemmas
1. Can Individuals Using Social Media be Data Controllers?
2. Intermediary Liability
3. Reliance on the Journalism Exemption or Freedom of Expression
IV. A Possible Role for Article 8 ECHR?
A. The General Relevance of Strasbourg Case Law
B. How Strasbourg's Article 8 Jurisprudence Might Apply
1. Data Dissemination Scenarios
V. Factors Going to the Weight of the Article 8 Claim and Their Possible Application to RTBF
A. The Nature of the Information
B. The Form of the Information: Images or Text?
C. Is the Data Subject a Public Figure?
1. The Importance of the "Public Figure" Criterion.
2. Strasbourg's Approach to "Public Figures"
3. Conceptual Problems with the "Public Figure" Doctrine
D. Prior Conduct of the Person Concerned as Waiving Their Right to Privacy
E. Circumstances in Which the Information Was Obtained
F. Does the Personal Data Relate to a Public or Private Location?
VI. Conclusion

I. Introduction

No-one living in a European Union country could fail to have noticed that on 25th May 2018, a new data protection regime came into force across the EU — the *General Data Protection Regulation*.[1] Work on the final stages of this article was punctuated by the constant arrival of "*GDPR* emails" from various organisations, imploring the authors to "stay in touch" by consenting to the continuing use of their contact details. As the emails piled up in inboxes, *GDPR* jokes proliferated on Twitter.[2] But beyond the mundane requirements of ensuring some control for the storing of personal data like email addresses, the *GDPR* introduced something both far more controversial but also shrouded in considerable mystery: an explicit "right to be forgotten" ("RTBF").[3] As is well known, a limited right along these lines derives from a famous case decided by the Court of Justice of the European Union ("CJEU"): *Google Spain SL v Agencia Española de protección de Datos,* which interpreted the right to erasure under the previous *Data Protection Directive 1995* so as to give individuals rights in relation to search indexing.[4] This has given rise to (at the last count) 680,000 requests for delisting, which have led to over 1.8 million URLs being removed from search results, amid

1. EC, *Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [*GDPR*]. The *GDPR* replaced the previous Data Protection Directive 95/46 EC [*1995 Directive*].
2. Martin Belam, "Businesses Resort To Desperate Emailing as GDPR Deadline Looms" *The Guardian* (24 May 2018), online: The Guardian <https://www.theguardian.com/technology/2018/may/24/businesses-resort-to-desperate-emailing-as-gdpr-deadline-looms>
3. *GDPR, supra* note 1, art 17. This goes considerably further than the right to erasure in Article 12(b) of the *Directive*, *supra* note 1.
4. *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (13 May 2014), C-131/12, ECLI:EU:C:2014:317 (CJEU) [*Google Spain*]. The right to erasure appeared in the previous *1995 Directive*, *supra* note 1, art 12(b); the judgment also referenced the right to object in Article 14.

considerable controversy.[5] However this right was limited — at least in the original judgment — to requesting Google and other search engines to de-list certain search results: *Google Spain* did not itself cover the right to request the deletion of actual content.[6] Hence while that decision was controversial world-wide,[7] the *GDPR*, in introducing a more detailed,

5. Daphne Keller, "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation" *Social Sciences Research Network* (22 March 2017), online: SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684> at 25 [Keller, "Right Tools"]. The searches referred to are those made under an individual's name.
6. See Keller, "Right Tools", *supra* note 5 at 34–35 citing Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales C-131/12"*, (2014) 14/EN (WP 225) at 2, online: <http://www.dataprotection.ro/servlet/ViewDocument?id=1080> [Article 29 Google Spain Guidelines] (Keller has pointed out that "data protection regulators have said that Google de-listings do not significantly threaten [free speech] rights, precisely because information is still available on the webpage"). However, as David Erdos has noted, there have been several judgments at the domestic level applying *Google Spain* that *have* resulted in deletion of substantive content: for examples see David Erdos, "Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU *acquis*" (2018) International Journal of Law and Information Technology 1–37 [Erdos, Intermediary Publishers].
7. See e.g. Eduardo Ustaran, "The Wider Effect of the 'Right to Be Forgotten' Case" (2014)14:8 Privacy & Data Protection 8; Paul Bernal, "The Right to Be Forgotten in the Post-Snowden Era" (2014) 5:1 Privacy in Germany (10 August 2014), online: PinG <www.pingdigital.de/ce/the-right-to-be-forgotten-in-the-post-snowden-era/detail.html>; Daniel Solove, "What Google Must Forget: The EU Ruling on the Right to be Forgotten", *LinkedIn* (13 May 2014), online: LinkedIn <https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten>.

comprehensive and explicit RTBF, will be more contentious still.[8] It should be of interest to Canadians, for two reasons. First, the *GDPR* has extra-territorial effect:[9] it will apply to entities based outside the EU that provide services to EU citizens involving the processing of their personal data. As is well known, *Google Spain* applied EU data protection law to Google, on the basis that it had a subsidiary base within the EU. But second, a Canadian version of RTBF is in the offing: the Office of the Privacy Commissioner of Canada recently concluded that such a right[10] already exists in Canadian law.[11] Canadian regulators and courts applying this right may well draw inspiration from European case law and regulatory practice arising under Article 17.

But what does the new provision actually mean, how will it work and how will it be reconciled with freedom of expression? Answers to these questions are far from easy, in part because scholars are only just starting to grapple with the new regime. As leading commentator Daphne Keller puts it, while "oceans of scholarly ink have been spilled discussing the

---

8. For reaction so far see e.g. Meg Ambrose, "It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten" (2013) 16:2 Stanford Technology Law Review 369; Jeffrey Rosen, "The Right to be Forgotten" (2012) 64:88 Stanford Law Review Online; Diane Zimmerman, "The 'New' Privacy and the 'Old': Is Applying the Tort Law of Privacy Like Putting High Button Shoes on the Internet?" (2012) 17:2 Communications Law and Policy 107; Paul Schwartz, "The EU-US Privacy Collision: A Turn to Institutions and Procedures" (2013) 126:7 Harvard Law Review 1966.
9. *GDPR*, *supra* note 1, recital 3, art 3(1) and 2(1)(a) (it applies to "the processing of personal data of data subjects who are in the [EU] by a controller or processor not established in the Union, where the processing activities are related to … the offering of … services … to such data subjects in the [EU]" at art 3(2)(a).
10. That is a right both to require search engines to 'de-index' certain results *and* to require individual websites to take data down.
11. See e.g. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5; and Office of the Privacy Commissioner of Canada, "Draft OPC Position on Online Reputation" (26 January 2018) online: OPC <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801>.

Google Spain case … the same cannot be said of the … *GDPR*".[12] But this is also because major questions generated by the new regime remain beset by uncertainty. As Keller puts it: "[e]ven Data Protection experts can't say for sure how the *GDPR* answers hugely consequential questions, like whether hosting platforms [such as Twitter, Facebook, YouTube and Tumblr] must carry out RTBF removals",[13] partly because of the sometimes "opaque" drafting of the *GDPR*.[14] There is also ambiguity around how far individuals using social media may themselves become fixed with obligations under the *GDPR*.[15]

These questions are important because the record of de-listing requests made under *Google Spain* gives us good reason to believe that social media companies will be a key target for Article 17 requests: George Brock found that "[t]he eight sites for which Google receives the most requests are either social media or profiling sites" and of these, requests to delink to Facebook posts have been the single largest category, with "some 130,000 Facebook links … removed from view" by May 2016.[16] Hence the question of whether individuals and social media platforms should be treated as data controllers will very quickly assume great practical importance. Both groups, if exposed to potential data protection obligations, will also want to know whether they can claim the benefit of the broad, "journalistic" exemption.[17] Ordinary people will also want to know if they can at least claim their own freedom of expression as a defence, even if they cannot claim to be acting for journalistic purposes. These major uncertainties have not comforted

12. Keller, "Right Tools", *supra* note 5 at 26.
13. *Ibid* at 30.
14. *Ibid* at 31.
15. See below, Part III.C.1.
16. George Brock, *The Right to be Forgotten: Privacy and the Media in the Digital Age* (London: IB Tauris, 2016) at 51.
17. There are four "special purposes" under which national law may grant exemptions from *GDPR* obligations under Article 85(2); the others being "academic", "literary" and "artistic" purposes. Either or both of the "academic" and "journalistic" exemptions may be relevant to academics blogging and using social media to promote and discuss their areas of research. See further below at 24, and Part III.C.3.

those expressing strong concern about the possible impact of all this on online freedom of expression, especially what some commentators have analysed as structural and procedural features that will push online intermediaries like Google and Facebook in the direction of acceding to RTBF requests even when unsound.[18] It is possible that national courts and legislatures, under pressure from media and the web giants, may seek to ameliorate the likely effect of the *GDPR* on their operations. Some national courts have at times been ready to cut down sharply the scope of key data protection definitions — such as "personal data" — in order to limit the impact of EU data protection rules on national law.[19]

There is clear guidance from the CJEU that EU data protection law must be interpreted and applied in a way that respects the "fundamental rights of the [EU] legal order"[20] which now include the basic rights to privacy, data protection and freedom of expression in the European Union Charter on Fundamental Rights.[21] Moreover, crucially, for the purposes of this article, the Court has said that guarantees in the Charter that are cognate to those in the European Convention on Human Rights ("ECHR") must be interpreted so as to give them "the same meaning and scope"[22] as the ECHR rights — in this case the more long-standing

18. See e.g. *infra* note 157.
19. For example, the UK Court of Appeal interpreted the notoriously broad concept of "personal data" narrowly by finding that whether an individual's data constitutes personal data depends inter alia on whether it is "information that affects his privacy, whether in his personal or family life, business or professional capacity" see *Durant v Financial Services Authority*, [2003] EWCA Civ 1746 at para 28.
20. *Lindqvist v Aklagarkammaren I Jonkoping*, C-101/01, [2003] ECR at I-12992 [*Lindqvist*].
21. EC, *Charter of Fundamental Rights of the European Union*, [2000] OJ, C 364/01 [EU Charter] (Articles 7, 8, and 10 protecting, respectively privacy, data protection and freedom of expression).
22. *Philip Morris Brands SARL v Secretary of State for Health*, C-547/14, [2016] ECLI:EU:C:2016:325 (CJEU); see also *Bernard Connolly v Commission of the European Communities*, C-274/99, [2001] ECR I-1638 at paras 37–42; see also Article 52(3) of the EU Charter, below at 40.

ECHR rights to privacy and freedom of expression.[23] Hence an important guide to the meaning of Article 17 is likely to be the jurisprudence of the European Court of Human Rights in Strasbourg ("the Strasbourg Court"). This is particularly so given that, as Keller observes, "[c]ases balancing rights to expression versus privacy … exist — but those rarely involve Data Protection, or set out rules for [online service providers], as opposed to ordinary publishers or speakers."[24] The one decision Keller cites here is the leading Strasbourg decision of *Von Hannover v Germany*[25] — which involved a traditional privacy claim against the print media. Hence a key enterprise of this paper: to try to figure out how the newly-formulated right to be forgotten will apply to online expression by drawing out relevant principles from the privacy case-law of the Strasbourg Court and applying them to this new situation. We should stress that our endeavour is limited to how the primary right should be construed, whom it will bind and who may claim exemptions from it by reference to the countervailing right of freedom of expression or the journalistic exemption. We do not go on to consider the substantive *content* of the freedom of expression side of the balance:[26] that would

23. *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 arts 8–10 (entered into force 3 September 1953) [*ECHR*]. Article 8 provides: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence". The second paragraph provides for restrictions only as they are provided for by law, in pursuit of a legitimate aim, such as the prevention of disorder or crime, or "protection of the rights and freedoms of others" and are necessary to protect these other rights or interests, which imports a proportionality test. Article 10 provides in para 1 that "Everyone has the right to freedom of expression"; the second paragraph provides a similar set of exceptions to para 2 of Article 8.
24. Keller, "Right Tools", *supra* note 5 at n 186.
25. No 59320/00, [2004] VI ECHR 41 [*Von Hannover*].
26. On balancing speech and privacy rights under the ECHR see, generally, e.g. Helen Fenwick & Gavin Phillipson, *Media Freedom Under the UK Human Rights Act* (Oxford: Oxford University Press, 2006) ch 1–2, 15; Eric Barendt, "Balancing Freedom of Expression and Privacy: The Jurisprudence of the Strasbourg Court" (2009) 1:1 Journal of Media Law 49.

require a separate paper.

This article is structured as follows. Part II will first sketch the challenges our contemporary online environment poses to traditional notions of privacy and explain how the RTBF offers the potential for greater privacy protection; in doing so it will answer some common objections to the notion of seeking to protect the privacy of users who themselves frequently disclose aspects of their own private life online. Part III will then set out the basic right under Article 17 and place it within the framework of the *GDPR*; it will consider some key interpretive questions that arise, including the potential legal responsibilities as "data controllers" of individuals and social media platforms under the *GDPR* and whether they may invoke the defence of freedom of expression and/or "journalistic purposes" when doing so. Part IV will introduce Strasbourg's "reasonable expectation of privacy" test and the multiple different ways it could be applied to the right to be forgotten, depending on the circumstances in which the right is invoked. Part V will then move on to consider the individual factors the Strasbourg Court employs when assessing whether a reasonable expectation of privacy exists and its strength — a crucial factor when it comes to balancing privacy claims against competing free expression interests. The following factors will be discussed: (a) the content of the data; (b) its form; (c) whether the data subject is a public figure; (d) implied "waiver" of privacy rights; (e) how the data was collected and disseminated; (f) whether the data relates to something that occurred in a physically public location.

II. Social Media and Self-Disclosure: The Abandonment of Privacy Online?

A. Why the Need for a Right to be Forgotten?

The right to erasure was formulated with the clear view of enhancing data privacy rights for EU citizens.[27] It is thus a considered response to technological advances that have resulted in "personal information being posted online at a staggering rate",[28] driven by the increasing prominence of social networking sites,[29] a digitised media,[30] cloud computing[31] and the widespread usage of websites in relation to professional life,[32] dating,[33] and sex.[34] A recent article noted that everyday 1.18 billion people will log into their Facebook accounts, often sharing both their own and other's personal data, 3,500 million tweets will be sent, 95 million photos and videos will be posted on Instagram and Youtube content creators will upload 72 hours of new video every minute.[35] A book published in 2014 recorded that Google processes, worldwide, over 3.5 billion searches a day. It adds, "the company had been in business more than a decade before it admitted that it had stored a record of every search ever

27. Viviane Reding, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" *European Commission Press Release Database* (22 January 2012), online: European Commission <http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm>.
28. Daniel J Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 19.
29. 2.46 billion people worldwide now use social networking sites: see e.g. *Statista*, online: Statista <https://www.statista.com/topics/1164/social-networks/>.
30. See e.g. *BBC News*, online: BBC <www.bbc.co.uk/news>.
31. See e.g. *Apple's iCloud*, online: Apple <www.apple.com/uk/icloud/>.
32. See e.g. *LinkedIn*, online: LinkedIn <https://gb.linkedin.com/>.
33. See e.g. *Eharmony*, online: Eharmony <www.eharmony.co.uk/home/rh-seo/>; *Match*, online: Match <https://uk.match.com/>.
34. See e.g. *Tinder*, online: Tinder <https://www.gotinder.com/>.
35. Max Mills "Sharing Privately: the Effect Publication on Social Media Has on Expectations of Privacy" (2016) 9:1 Journal of Media Law 45.

requested".[36] What Solove calls "generation Google"[37] became familiar from an increasingly young age[38] with internet-enabled smartphones and tablets that can take, store and upload photographs in seconds, allowing for highly impulsive sharing. Meanwhile the popularity of blogging and vlogging, including by minors, continues to grow, with one study finding that many are more akin to "personal diaries" (37%) rather than being devoted to topics like politics (11%). Solove comments:

> As people chronicle the minutia of their daily lives from childhood onwards in blog entries, online conversations, photographs, and videos, they are forever altering their futures – and those of their friends, relatives, and others.[39]

Mayer-Schönberger's seminal work, *Delete*, drew attention to the risks of a "loss of forgetting" in the digital age, with the huge quantity of personal data now "remembered" online, due to the "perfect recall" of the internet, threatening to reduce the personal autonomy of individuals and their ability to "move on" in their lives.[40] As Solove puts it, people want the option of "starting over, of reinventing themselves" but may nowadays be hampered in doing so by their "digital baggage".[41] In this regard search engines play a crucial role, rendering information on incidents that happened years ago instantly retrievable world-wide. One author gives the example of a student posting on a blog that she spotted her teacher in a gay bar; when that kind of gossip circulated in hard copy

36. Brock, *supra* note 16 at 20.
37. Daniel Solove, "Speech, Privacy, and Reputation on the Internet" in Saul Levmore & Martha Nussbaum, eds, *The Offensive Internet: Speech, Privacy, and Reputation* (Cambridge, Mass: Harvard University Press, 2010) 17 [Solove, "Speech, Privacy"].
38. See e.g. Ofcom, "Children and Parents: Media Use and Attitudes Report" (October 2014), online: Ofcom <stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-use-attitudes-14/Childrens_2014_Report.pdf> (stating that almost 8 in 10 children aged 12–15 own a mobile phone and there has been an increase since 2013 in those children using such phones to go online).
39. Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press: 2007) at 24.
40. Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press: 2009).
41. Solove, "Speech, Privacy", *supra* note 37 at 18.

student gossip sheets, it would have been buried in obscurity within a few months. Nowadays, "a person thinking of hiring the teacher twenty years later" can find that information "with just a few keystrokes".[42]

B. Theoretical Dimensions

We have thus far suggested that this explosion of personal data online, and the harm it can do, shows why we need a right to delete. However we must at this point consider a commonly advanced objection: that, not only has the internet rendered privacy laws more difficult to enforce but that the behaviour of people online shows that people today — particularly, it is said, young people — proves that they value self-expression, or "transparency *over* informational privacy".[43] It is certainly a common trope to bemoan the prevalence of "young people who behave as if privacy doesn't exist"[44] or they "don't care" about it.[45] When the Pew Foundation canvassed the views of experts, one wrote "[w]e have seen the emergence of publicity as the default modality"[46] while the Foundation summed up their collective view as being that "privacy [is] no longer a 'condition' of American life".[47] In order to respond to this argument it is

42. Geoffrey R Stone, "Privacy, the First Amendment, and the Internet" in Saul Levmore & Martha Nussbaum, eds, *The Offensive Internet: Speech, Privacy, and Reputation* (Cambridge, Mass: Harvard University Press, 2010) 192.
43. *Ibid* at 193 (emphasis added).
44. Emily Nussbaum, "Say Everything" *New York* (12 February 2007), online: New York <nymag.com/news/features/27341/>.
45. See e.g. Irina Raicu, "Young adults take more security measures for their online privacy than their elders" *recode* (2 November 2016), online: recode <https://www.recode.net/2016/11/2/13390458/young-millennials-oversharing-security-digital-online-privacy>; see also Lee Rainie, "The state of privacy in post-Snowden America" *Pew Research Center* (21 September 2016), online: Pew Research Center <www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>.
46. Lee Rainie & Janne Anderson "The Future of Privacy" *Pew Research Center* (8 December 2014) quoting Stowe Boyd, online: Pew Research Center <www.pewinternet.org/2014/12/18/future-of-privacy>.
47. *Ibid*.

necessary to recall some basics from the theoretical literature on privacy.[48] We make no attempt to add substantively to that already copious literature: our aim is simply to highlight the relevance of a key distinction that is in danger of being forgotten in this discussion. In summary our argument is that views like the above may tempt us to overlook a fairly fundamental distinction: between privacy as a state-of-being, and privacy as a *claim:* a moral claim, that can also be a legal one.

What is the essence of this distinction? The starting point is that privacy as a state-of-being is *descriptive*; privacy as a claim is *normative*. As a description of privacy, we consider that one of the most compelling comes from the scholarship of Ruth Gavison[49] and Nicole Moreham:[50] that privacy is a state of "desired in-access to others".[51] "Access" to a person can obviously occur on a number of different levels: through touch, through sight (a peeping Tom), through hearing (by someone eavesdropping on a private conversation), through intrusion into our physical space (someone coming uninvited into your garden or home), or through a person accessing personal information about us (by reading our emails or other online private content). The argument in short is that our privacy depends upon the extent to which others can see or access us. This is why — to give simple examples — we have locked doors for toilets, and why we do not, by and large, undress in public: locked doors and clothes alike put some barriers in the way of the visual access others

48. For a major recent work on privacy in a networked world see Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012).
49. Ruth Gavison, "Privacy and the Limits of the Law" (1980) 89:3 Yale Law Journal 421.
50. Nicole Moreham, "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121:4 Law Quarterly Review 628. For an account along broadly similar lines, see also RB Parker "A Definition of Privacy" (1974) 27:2 Rutgers Law Review 275.
51. The "desired" element of course is to distinguish enjoying privacy from being marooned on a desert island, or in solitary confinement desperate for any human contact — it would be odd in such situations to describe someone as being in a state of perfect privacy: see e.g. Moreham, *ibid* at 636, *et seq.*

have to us.[52] We may also seek to bar access not to our writings but our *identities*, as where people blog anonymously online,[53] a classic example of the key online phenomena Mills calls "sharing privately". [54] A well-known key effect of the internet is that the unwanted access to us that one or two people might obtain in the physical world (through prying or eavesdropping) can be instantaneously granted to millions of others — when images or recordings of a person are posted online. The online world therefore poses the "insidious threat that information shared has the capacity to be disseminated further, throughout social networking sites and even reaching mass media".[55] The literature is full of examples: an extreme one concerns a girl who, back in 2000, made intimate videos for her boyfriend of her stripping and masturbating; they were placed online by persons unknown and became some of the first "viral videos", turning her into an accidental online porn star, with her own Wikipedia entry.[56]A more mundane example is the *Daily Mail* publishing Facebook photos of drunken "girls' nights out" to a mass audience under the headline: "The ladettes who glorify their shameful antics on Facebook".[57]

The above discussion shows how a key contemporary concern is that greater access to the *informational* dimension of our private sphere will

52. Kirsty Hughes analyses such behaviour as the placing of "privacy barriers" in the way of others; invasions of privacy occur when such barriers are breached: see Kirsty Hughes, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" (2012) 75:5 The Modern Law Review 806.
53. For a decision that failed to recognise the vital privacy-based interest in anonymous blogging see *The Author of a Blog v Times Newspapers Ltd*, [2009] EWHC 1358 (QB).
54. Mills, *supra* note 35 at 46.
55. *Ibid.*
56. Nussbaum, *supra* note 44.
57. Andrew Levy, "The ladettes who glorify their shameful drunken antics on Facebook" *Mail Online* (5 November 2007), online: Mail Online <www.dailymail.co.uk/news/article-491668/The-ladettes-glorify-shamefuldrunken-antics-Facebook.html>. Multiple extreme examples of such persecutory and harassing speech are discussed by Danielle Citron in *Hate Crimes in Cyberspace* (Cambridge, Mass: Harvard University Press, 2016).

diminish our privacy as a state-of-being. In response to this concern, people put forward a *claim* to privacy. Many have argued that this is best captured as being a claim for *control* over our personal information:[58] that it is up to the individual how much of their private sphere — including information — they choose to share with others. Certainly, the notion of informational autonomy is the easiest to apply to the regulation of online privacy: both the EU and Strasbourg Courts have recognised it as a key value underlying both data protection and Article 8 ECHR. Recital 7 of the *GDPR* states that, "[n]atural persons should have control of their own personal data";[59] the Strasbourg Court recently observed that Article 8 ECHR, the right to privacy, "provides for the right to a form of 'informational self-determination'".[60] It is when that control is *taken from* individuals — revealing images of them are posted online, their phone is

58. Alan Westin, *Privacy and Freedom* (London: The Bodley Head Ltd, 1970) (Westin has argued that "privacy is the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others" at 7); see also Alan Westin, "The Origins of Modern Claims to Privacy" in Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984) 56; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto: Stanford University Press 2009); Paul Gewirtz, "Privacy and Speech" (2001) 2001:1 The Supreme Court Review 139; Charles Fried, "Privacy" (1968) 77:3 Yale Law Journal 475, esp 482–43; Solove, "Speech, Privacy", *supra* note 37 at 21 (Solove uses practical examples to show the keen desire for control over accessibility: over 700,000 people complained to Facebook when it introduced News Feed, alerting people's friends when their profile was changed or updated even though many of the complainants had publicly available profiles).
59. *GDPR*, *supra* note 1, recital 7.
60. *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,* No 931/13 (27 January 2017) [*Satakunnan*].

hacked,[61] their email and telephone records accessed by government,[62] or photos taken of them coming out of a drug treatment facility[63] — that we can say their privacy has been "invaded".

From this one initial point emerges: while people can choose to give others greater or lesser "access" to their personal sphere, they cannot — as tabloid editors are prone to say as justification for publishing intrusive stories about publicity-seeking celebrities — "invade their own privacy". It is only when someone's control over their private sphere is *taken from* them that their privacy is *invaded*. That is, at least, the "old media" perspective. Applying this insight to *social* media is slightly more complex — but of far more universal application: it applies to all of us who post some kind of personal information online. It is true that our behaviour in doing this may show a very different attitude to privacy from that of our parents' or grandparents' generation;[64] this leads to the argument, noted above, that such behaviour shows that people nowadays care more about transparency and expression than privacy.

To address this argument, we must consider the complex relationship between the needs of self-expression and sociability and of privacy, used in a descriptive sense. We draw close to people by giving them access to us — to our thoughts, our vulnerabilities, homes, or personal space; in the case of sex and love, to the most intimate parts and aspects of ourselves. What we do appear to have seen in the last few decades

---

61. See e.g. UK, Leveson Inquiry, *An Inquiry into the Culture, Practices and Ethics of the Press* by The Right Honourable Lord Justice Leveson: Report, (London: Her Majesty's Stationery Office, 2012) (concerns about press practices such as blagging and hacking led to the Leveson Inquiry as well as numerous civil cases against newspapers, most of which were settled).
62. In the UK the revelation of the bulk collection of communications data by the state led eventually to the decision in *Secretary of State for the Home Department v Watson MP*, [2018] EWCA Civ 70 finding the then regulations unlawful: they have been replaced with permanent, sweeping statutory powers under the *Investigatory Powers Act* 2016.
63. As in the leading UK decision of *Campbell v MGN Ltd*, [2004] UKHL 22 [*Campbell*].
64. See Nussbaum, *supra* note 44, for a range of extreme examples of self-disclosure.

is a shift in the relative value people give to privacy as state-of-being, compared to the value they attach to self-expression online as a means of connecting with people. Some people undoubtedly use social media to do this in a rather undifferentiated way: for example, seeking approval for their physical appearance from an online mass audience, instead of a few close friends.[65]

However — and this is our key point — none of this means that people do not still value the *right* to privacy: they still want to decide *what* and *how much* they share — even if some use that choice to share far more with far more people than their parents would have dreamt of doing. A recent research project by the Pew Foundation found that "74% [of Americans] say it is 'very important' to them that they be in control of who can get information about them".[66] We see this in increasing concern and awareness about things like the "privacy settings" on Facebook,[67] how far people really give consent to the volume of information they are sharing with Google (which knows all the searches you've made) or Amazon or Kindle (which knows which of their books you have read); or Gmail, which has all the emails you've sent.[68] Different people will always draw this boundary differently and that in itself is no cause of concern: in the "offline" world we will all know some people who are quite reserved — sharing aspects of their private life with only a few

65. An extreme example is the phenomena of "ratings communities", like "nonuglies", where people post photos of themselves to be judged and rated by strangers. See Nussbaum, *ibid*, for these and other examples and e.g. <https://www.livejournal.com/blogs/en/nonuglies>.

66. Lee Rainie, "The State of Privacy in Post-Snowden America" *Pew Research Center* (21 September 2016), online: Pew Research Center <www.pewinternet.org/2014/12/18/future-of-privacy/>. While such control can be argued to have good *consequences* it can also be seen in deontological terms as an aspect of human dignity; for a classic account see Edward J Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39:6 New York University Law Review 962.

67. See e.g. Solove, "Speech, Privacy", *supra* note 37 at 21, discussed *supra* note 58.

68. For a recent major work on this subject see Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford: Oxford University Press, 2015).

trusted friends — and others, who will drunkenly share intimate details of their love-lives with near-strangers. Privacy boundaries vary greatly between different societies; even *within* given societies, they will vary greatly between individuals and be drawn and re-drawn repeatedly. All that we can generalise is that it is a pervasive feature of human relations that, as Solove puts it, most people "reveal information to certain groups while keeping it from others".[69]

A key point therefore is that, while the boundaries between self-expression and privacy will always vary between people and shift as society changes, none of that means that individuals should be deemed to have given up the core *right to privacy* — the claim that is, to exercise some control over access to their inner sphere, and particularly, their personal information. To argue that someone who chooses to share a great deal of their private information with others online, for that reason becomes fair game to have their private information taken from them without their consent, is a little like arguing that a woman who chooses to share her body intimately with many others by having numerous transitory sexual partners should lose her right to choose with whom she has sex.[70]

That then is the core response to the argument that the proliferation of intimate personal information placed voluntarily online provides a reason against allowing legal claims for invasion of privacy when such information is used *in*voluntarily. But there is a further point, also a well-known argument, but we think particularly apt in the case of social media. While the press and much scholarship, particularly from US First Amendment scholars, tends to portray privacy and self-expression as invariably in tension,[71] they also go hand-in-hand. Privacy, as Fried has argued, is essential to the intimate communication vital to fostering

---

69. Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 42–4.
70. We do not of course suggest that the scale of violation in the two cases is comparable, merely the way in which, in both cases, past behaviour is used to justify dispensing with consent.
71. See e.g. Diane Zimmerman, "Requiem for a Heavyweight: a Farewell to Warren and Brandeis's Privacy Tort" (1983) 68:3 Cornell Law Review 291; Richards, *supra* note 68.

close relationships: most of us will only share information that might be deeply painful or simply embarrassing with a friend or partner *if* we are reasonably sure that they will keep it to themselves; hence an assurance of privacy can actually ensure greater self-expression between people and thus greater intimacy.[72] Online, this often translates into the need for anonymity, in which guise it facilitates individual self-exploration in the form of reading, watching and listening to a wide range of media often shared on social media, as well as blogging on intimate subjects. For example a deeply-conservative Evangelical Christian, seeking to explore his possible homosexuality is likely to do so online only if fairly sure that he can keep his explorations to himself. Exactly the same argument applies to the personal blogs that abound on the internet. This is what De Cew calls "expressive" privacy — "a realm for expressing one's self-identity or personhood".[73] This dimension of privacy then is crucial to individual self-development, exploration and self-actualisation: all values commonly argued to underlie free speech.[74]

Thus as Mayer-Schönberger has pointed out, the purpose of the right to delete is to combat the loss of control an individual faces when their information and history — in a very real sense their personal identity — becomes, in Bernal's words, "an indelible part of a mass of information usable and controllable by others".[75] However, the notion of a right to delete should also change the way the concept of informational autonomy is applied in privacy cases. Under the "old-media" paradigm, previous self-publicity could be treated as a "waiver"

---

72. See Charles Fried, "Privacy" (1968) 77:3 The Yale Law Journal 475; for a similar argument, see Jeffrey Reiman, "Privacy, Intimacy, and Personhood" (1976) 6:1 Philosophy & Public Affairs 26.
73. Judith W DeCew, "The Scope of Privacy in Law and Ethics" (1986) 5:2 Law and Philosophy 145, at 166, also see 167–170.
74. For classic accounts see Frederick Schauer, *Free Speech: A Philosophical Enquiry* (Cambridge: Cambridge University Press, 1982); Kent Greenawalt, "Free Speech Justifications" (1989) 89:1 Columbia Law Review 119; Eric Barendt, *Freedom of Speech*, 2d ed (Oxford: Oxford University Press, 2005) ch 1.
75. Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge: Cambridge University Press, 2014) at 206.

of privacy rights,[76] under which an individual's prior decision to speak to the press about an aspect of their private life could lead to courts finding they had lost their previous reasonable expectation of privacy. Such loss could apply to the whole of their personal life (under the extreme notion of a "blanket waiver") or just the same broad area (e.g. sex-life) that they had previously publicised.[77] This approach comes close to treating informational autonomy as a one-off event: the individual gets to choose *once* whether to share certain personal information with a large audience. Then precisely *because* they made that choice, they are deemed to have *lost* the right to exercise it later. That approach always contradicted the premise of the informational autonomy model but it was one that media organisations successfully persuaded at least some courts to adopt. But the right to delete inescapably insists on a different approach, under which the right to control over personal information is not a one-off, but something that one can exercise *continuously*; thus, information one had previously publicised could still be the subject of a deletion claim. The notion that control is "waived" by self-publicity is necessarily rejected as incompatible with any meaningful right to delete. Thus, RTBF requires a shift in our understanding of informational self-determination, from being (potentially) a one-off event, whereby control is exercised, but simultaneously lost for the future, to being instead a *continuing* entitlement.

In short, privacy in a socially-networked world is about degrees of control over information about ourselves and determining the degree and nature of social interaction with others. If we lose that control we become

76. See e.g. *infra*, text following note 256; for a critique of the concept of "waiver" see Gavin Phillipson, "Press Freedom, the Public Interest and Privacy" in Andrew Kenyon, ed, *Comparative Defamation and Privacy Law* (Cambridge: Cambridge University Press 2016) at 150. In the US context, celebrities may be seen to have waived their right to privacy; thus giving media bodies a claim of "implied consent" to privacy claims brought against them: see e.g. John P Elwood, "Outing, Privacy and the First Amendment" (1992) 102:3 Yale Law Journal 747.

77. Known as the "zonal approach": for examples, see e.g. *Douglas v Hello!*, [2003] 3 All ER 996 (CA) at para 226 (sex life) and *A v B*, [2005] EWHC 1651 (QB) (drug use).

"powerless objects available for capture", a mere "bundle of details, distortedly known, presumptuously categorised, instantly retrievable, and transferable to numerous unspecified parties at any time"'.[78] The right to delete is part of the attempt to re-empower us online; all of us. Because, unlike classic tort privacy actions, which are typically available only to the wealthy celebrities who can afford them, RTBF is a remedy that anybody can use — hundreds of thousands have already.[79]

III. The Right to be Forgotten: Key Interpretative Issues

A. The Focus of This Article

This article considers RTBF only in relation to what we might broadly term online expression: by this we include traditional media online, such as newspaper and news websites, but also social media, search engines, blogs and all the other now-familiar aspects of Web 2.0. We are not therefore concerned with relatively uncontroversial aspects of RTBF, such as requiring the deletion of ordinary commercially-valuable personal data like contact details from a company whose services we previously used, or of personal data held by employers or public bodies, like health services and law-enforcement agencies. Nor, in relation to social media platforms will we consider what Keller terms "back-end data", that is, data that online service providers (OSPs) themselves collect "by tracking their own users' online behaviour"[80] such as clicks, "likes", etc., in order to target advertisements at them. As straightforward commercial data we do not treat this as an aspect of online expression (though it undoubtedly raises privacy concerns). Hence, when we discuss RTBF we are concerned *only* with its use in respect of data placed online by another individual or media body, whether the data subject themselves or a third party. Finally,

78. Anne SY Cheung, "Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd" (2009) 1:2 Journal of Media Law 191 at 210. See also Beate Rossler, *The Value of Privacy*, translated by RDV Glasgow (Cambridge: Polity Press, 2005) at 106.
79. See above, at 3.
80. Keller, "Right Tools", *supra* note 5 at 4.

we are not concerned with scenarios in which an individual uploads their own personal information (such as photographs) to a social networking site like Facebook *but* retains first-hand control over it: since they are at liberty simply to delete it from the site (or even close their account completely),[81] they would not need to invoke Article 17. However, if that data has subsequently been copied or shared such that it is now beyond the individual's control, that takes us into scenarios that we do consider.

B. Article 17 *GDPR*: The Basics

Article 17 gives the right to "data subjects" (an identifiable natural person to whom information online relates);[82] it lies *against* "data controllers" — those who "alone or jointly with others, determine the purposes and means of the processing of personal data";[83] this likely includes, for example, website hosts, authors of certain web-pages and search engines.[84] "Processing" is very broadly defined and includes "collection … storage … retrieval … use … disclosure by transmission, dissemination or otherwise making available"[85]; hence it plainly encompasses the publication of personal data online, in whatever form. As discussed at various points below, the *GDPR*, in common with the earlier *Directive*, affords particular protection to what was previously known as "sensitive personal data", now referred to as "special category data" (the former term will be used as the more intuitive match). This is defined in Article 9(1) as personal data revealing:

> racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or

81. See Sophie Curtis, "How to permanently delete your Facebook account" *The Telegraph* (19 August 2015), online: The Telegraph <www.telegraph.co.uk/technology/facebook/11812145/How-to-permanently-delete-your-Facebook-account.html>.
82. *GDPR, supra* note 1, art 4.
83. *Ibid,* art 4(4).
84. *Google Spain, supra* note 4 (the CJEU found that Google was a data controller; the definition in *GDPR*, Article 4 is virtually the same as that considered in *Google Spain*).
85. *GDPR*, *supra* note 1, art 4(2).

> … a natural person's sex life or sexual orientation.[86]

While Article 9(1) appears baldly to prohibit the processing of such data, there are broadly worded exceptions; these include the "explicit consent" of the data subject,[87] where the data subject has "manifestly made the data public"[88] and where:

> processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[89]

The *GDPR* is a Regulation and, as such, automatically applicable across all EU states without the need for domestic implementation; however, its provisions specifically allow for Member States to supplement it by domestic laws,[90] especially to provide exemptions to ensure proper protection for freedom of expression and information. Article 85(1) *GDPR* requires Member States "by law" to "reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information".[91] Article 85(2) more specifically states:

> For processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, Member States shall provide for exemptions or derogations from [key provisions of the *GDPR*] if they are necessary to reconcile the right to the protection of personal data with the freedom of

86. *Ibid*, art 9(1).
87. *Ibid*, art 9(2)(a).
88. *Ibid*, art 9(2)(e) (we are grateful to David Erdos for pointing out that the exception actually refers to data "which *are* manifestly made public" — the possible significance of this odd use of the present tense is considered further below at note 103).
89. *GDPR*, *supra* note 1, art 9(2)(g).
90. For a useful summary of these provisions see Daphne Keller, "The GDPR and National Legislation: Relevant Articles for Private Platform Adjudication of 'Right to Be Forgotten' Requests" *Inforrm* (5 May 2017), online: Inforrm <https://inforrm.org/2017/05/05/the-gdpr-and-national-legislation-relevant-articles-for-private-platform-adjudication-of-right-to-be-forgotten-requests-daphne-keller/>.
91. *GDPR*, *supra* note 1, art 85(1).

expression and information.[92]

The UK has just passed such legislation,[93] the *Data Protection Act 2018*[94], which grants sweeping exemptions from the key requirements of the *GDPR* and the remedies it grants — including Article 17 — for processing, including of sensitive personal data, done in pursuit of "the special purposes", including journalism.[95] Many EU countries, however, had not passed any such legislation by the time this article went to press; hence the concrete effect of the *GDPR* will probably take many years to become apparent and considerable variation is likely to be found amongst the Member States. Since this article concerns the *GDPR* itself, rather than law in the UK, only brief mention will be made of the *2018 Act*, for illustrative purposes.

Article 17, as material, provides:

> (1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
> > (b) the data subject withdraws consent on which the processing is based … [96] and where there is no other legal ground for the processing;

92. *Ibid*, art 85(2).
93. While the UK has decided to withdraw from the EU and will currently do so on 29 March 2019, it is legislating so as to retain the vast majority of currently applicable EU law in the *European Union (Withdrawal) Act 2018* (UK), c 16. While the bill specifies certain EU instruments that will *not* be retained, the *GDPR* is not one of them.
94. *The Data Protection Act 2018* (UK), c 12 [*2018 Act*].
95. See below, at 34.
96. *GDPR, supra* note 1 (the provision refers both to consent under Article 6(1) to the processing of "ordinary personal data" and "explicit consent" under Article 9(1) to the processing of "sensitive personal data").

> (c) the data subject objects to the processing pursuant to Article 21(1)[97] and there are no overriding legitimate grounds for the processing,
>
> (d) the personal data have been unlawfully processed; …
>
> (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).[98] …
>
> (3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
>
> (a) for exercising the right of freedom of expression and information …

It also contains a requirement for controllers to inform third parties who are processing the same data that it has been requested for deletion under Article 17(2).[99] As will be seen, the right is broadly framed, and does not appear to require any threshold of seriousness to be met in order to invoke it.[100] Given the reference to withdrawing consent, Article 17 *may* apply to information initially uploaded by the data subject themselves as well as that uploaded by a third party. As Recital 65 makes clear:

---

97. The right to object referred to is objection to processing "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" see *GDPR*, *ibid*, art 6(1)(f).
98. This means essentially that the information was collected from a child and they or their parents consented at the time (children may only consent from the age of 13 on). "Information society services" are defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service" see *GDPR*, *ibid*, art 8(1). They include online shops, streaming services and social media, see *GDPR*, *ibid*, art 4(25).
99. *GDPR*, *ibid*, art 17(2) provides: "Where the controller has made the personal data public and is obliged … to erase [it], the controller, taking account of available technology and the cost of implementation, shall take reasonable steps … to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data".
100. As opposed to, for example, a defamation claim brought in English law under the *Defamation Act 2013*, (UK) c 26 (see section 1).

> [T]he right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.[101]

The ability to use the right to delete in order to leave behind embarrassing childhood images or posts is one of the more widely-accepted aspects of RTBF. It should be noted that, in the case of material that was uploaded by the data subject as an adult, withdrawal of consent grounds a claim *only* where the previous consent of the data subject was the sole lawful basis for processing the data.[102] Thus for "ordinary data", the controller could rely instead on their "legitimate interests" (unless overridden by the privacy interests of the data subject) as a lawful basis for processing. If the data is "sensitive" within the meaning of Article 9, the controller could seek to rely on a deliberate decision by the data subject to make the data public[103] in the past, such as posting it to a public website as the basis. If this condition was found to be made out, then withdrawal of consent *per se* would not appear to ground a deletion request.

Finally, and very importantly, Article 17 makes clear that, even where paragraph (1) is satisfied, the right is only *prima facie* made out: it must then be balanced against freedom of expression of either or both of the data controller and (if the two are not the same) the original poster of the

---

101. *GDPR, supra* note 1, recital 65.
102. *Ibid*, art 17(1)(b).
103. *GDPR*, *ibid*, art 9(2)(e). As noted above, *supra* note 88, the wording of the *GDPR* refers to data "which *are* manifestly made public". In the UK context, the *2018 Act*, *supra* note 94, s 86(2) states that the processing of sensitive personal data "is only lawful" if "at least one condition" from both Schedule 9 *and* Schedule 10 is fulfilled. In many cases involving online expression the *only* likely condition that could be relied on in Schedule 10 is para 5: "The information contained in the personal data *has been made public* as a result of steps deliberately taken by the data subject" [emphasis added]. Evidently the effect of the UK legislation here might be different from the *GDPR* provision. How this situation would be resolved in other member states might turn on the particular terms of their own *GDPR* legislation.

data.[104] On the face of it, it appears therefore that freedom of expression could be invoked to refuse deletion as a particular remedy, even where the data being requested for deletion is being processed unlawfully. This might arise, for example, where the data requested for deletion is "sensitive" and there is no legal basis for processing it.[105]

C. Some Key Interpretive Dilemmas

As noted above, the *GDPR* leaves a number of extremely important issues unclear. Three in particular stand out: first, will private individuals uploading information about others online be classed as data controllers and hence subject to RTBF requests? Second, will social media platforms publishing such third-party content be controllers (often referred to as the "intermediary liability" issue)? And third, who will benefit from the broad exemption for "journalism"? As these issues are canvassed in detail elsewhere;[106] only a relatively brief account is offered here.

1. Can Individuals Using Social Media be Data Controllers?

We consider first the possible liability of individuals. Many might bridle at the notion that we "process the personal data" of others; however, most of us do it all the time. A very common scenario involves an individual

104. *GDPR*, *supra* note 1, art 17(3)(a).

105. We are indebted to David Erdos for pointing this out.

106. On the intermediary liability question see Keller, "Right Tools", *supra* note 5, and Erdos, "Intermediary Publishers", *supra* note 6; on the issue of individuals as possible data controllers see David Erdos, "Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication" (2017) 33:3 Computer Law and Security Review 275 [Erdos, "Domestic"]: Brendan V Alsenoy, "The Evolving Role of the Individual Under EU Data Protection Law" (2015) CiTiP Working Paper 23/2015, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641680>; on the scope of the journalist exemption see above Erdos, "Domestic" and David Erdos, "From the Scylla of Restriction to the Charybdis of License? Exploring the Present and Future Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection" (2015) 52:1 Common Market Law Review 119.

posting a photograph of a friend or family member, often showing the two of them together. If the post included a comment such as "Annabel had a bad dose of flu but still looked great!" then the poster has processed *sensitive* personal data about another. So, in scenarios like these, will the poster be counted, at least for some purposes, as a "data controller"? The so-called "household" exemption in the *GDPR* is the starting point. This provides that the Regulation "does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity".[107] Recital 18 explains that this means processing "with no connection to a professional or commercial activity"[108] and that such processing "*could* include … social networking and online activity undertaken within the context of such activities".[109] Research by David Erdos on the attitude of national Data Protection Authorities ("DPAs") across the EU showed wide variation in their approach to this issue; however, a common theme was that a key distinction was to be drawn between publication to a small, controlled group — likely to fall within the "household exemption" — and publication to an indefinite group, which would not. As Erdos puts it:

> The vast majority [of]… DPAs hold that once personal information relating to somebody other than the publisher themselves is disseminated to an indefinite number, the personal exemption cannot apply.[110]

It appears that this is based on the decision of the CJEU in *Lindqvist*,[111] interpreting an almost identical exempting provision in the previous 1995 *Data Protection Directive*. In that case, the Court said that the exemption was confined:

> only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.[112]

---

107. *GDPR*, *supra* note 1, recital 18.
108. *Ibid*.
109. *Ibid* [emphasis added].
110. Erdos, "Domestic" *supra* note 106 at 276.
111. *Lindqvist*, *supra* note 20.
112. *Ibid* at para 47.

This approach has been echoed by the EU's Article 29 Working Party ("Working Party")[113], which in 2013 said: "[i]f a user takes an informed decision to extend access beyond self-selected 'friends', data controller responsibilities come into force".[114] Thus under our scenario of posting a photo of Annabel, the crucial factor would be the privacy settings the poster was using: provided the photo was posted only to a closed group of "friends", the Household exemption would likely apply, meaning the *GDPR* would not. However, if it were posted to a *public* forum — as in a Facebook post made available to all, or a tweet — then the individual *would* become a data controller in respect of that item.

Erdos notes further that some DPAs took a more "stringent approach" suggesting that, in general, use of others' personal data on social networking sites should require data subject consent.[115] Conversely, one of the most permissive DPAs was the UK's Authority, which said that the personal exemption would apply:

> whenever someone uses an online forum purely in a personal capacity for their own domestic or recreational purposes; [hence it] will not consider complaints made against individuals who have posted personal data whilst acting in a

113. *Directive*, *supra* note 1, art 29 established a Working Party on the Protection of Individuals with regard to the Processing of Personal Data ("the Working Party"). In the first UK case of a *Google Spain*-style delisting that reached the courts, Warby J in the High Court said: "All parties are agreed that [Guidance by the Working Party on *Google Spain*] will be of the greatest use to me in assessing the claims" see *NT1 and NT2 v Google*, [2018] EWHC 799 (QB) at para 39 [*NT1*].

114. Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking*, (2009) 01189/09/EN (WP163) at 6. A subsequent report in 2013 suggested that such a factor should not be determinative but only be "an important consideration" amongst many see Article 29 Data Protection Working Party, *Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package*, (2013) Annex 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities at 9; but by 2015 the Working Party had seemingly returned to advocating only a narrow limitation see Article 29 Data Protection Working Party, *Appendix: Core Topics in View of the Trilogue*, (2015) Annex to the letters at 3.

115. Erdos, "Domestic", *supra* note 106 at 286. This group had 11 DPAs including from Norway, Germany, France, and Belgium.

> personal capacity, no matter how unfair, derogatory or distressing the posts may be.[116]

Erdos's own view suggests a more qualitative analysis whereby:

> the interpretation of the personal exemption should be widened to encompass those forms of individual publication which do not pose a serious *prima facie* risk of infringing … the core privacy, reputation and related rights which data protection is dedicated to safeguard.[117]

He suggests three situations in which such a risk would be present: (a) "clearly pejorative posts" (e.g. a student critiquing a particular teacher by name); (b) "disclosure of private details re private life (especially if sensitive)" or (c) comments that are "so frequent and focused" that they amount to harassment.[118] We argue below that in making such a qualitative assessment, guidance from the Strasbourg Court could play a useful role.

In short then, it is not possible to be sure either about the correct interpretation of the *GDPR* in this respect, *or* the practice of national DPAs with primary responsibility for enforcing it. It is likely that the major variations in approach identified by Erdos will continue for several years, at least until authoritative and detailed guidance is obtained from the CJEU or the new European Data Protection Board.[119]

2. Intermediary Liability

What then of the social media platforms themselves? Keller points out how a request by another for Twitter to erase a tweet that Keller had written:

> affects at least four key sets of rights: my rights to free expression, [the data subject's] rights to Data Protection and privacy, other Internet users' rights to

116. UK, Information Commissioner's Office, *Social networking and online forums – when does the DPA apply?* (2014), at 15 online: ICO <https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf>.
117. Erdos, "Domestic", *supra* note 106 at 276, 292.
118. *Ibid* at 292.
119. Established under *GDPR*, *supra* note 1, art 68, and tasked with, *inter alia*, providing best practice guidance regarding deletion requests see *GDPR*, *supra* note 1, art 71(1)(d).

seek and access information, and Twitter's rights as a business.[120]

It is important to note, that in EU law, the liability of such "hosts" for third party content that is (for example) in breach of copyright, is governed by the E-Commerce Directive;[121] this, broadly, shields hosts from liability in respect of such content in the absence of knowledge of its unlawfulness. However, despite some suggestions to the contrary[122] it seems tolerably clear that this regime will not apply to data protection claims[123] and that the *GDPR* will. The starting point is *GDPR* Recital 18, which, having granted the exemption for "purely personal", or "household" processing, immediately goes on: "this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities".[124] The Working Party in a recent opinion argued that *both* the social networks and the original poster would be data controllers in relation to material posted by users.[125] Erdos thinks it is clear that social media platforms like Facebook[126] *will* be data controllers; this would be consistent with the E-Commerce Directive, he contends, as the primary obligations will be ex-post obligations to remove data once their attention is drawn to it (including the right to delete). This, he

120. Keller, "Right Tools", *supra* note 5 at 18–19.
121. EC, *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, [2008] OJ, L-178 [E-Commerce Directive].
122. Especially by Keller, "Right Tools", *supra* note 5.
123. E-Commerce Directive, *supra* note 121, recital 14, seems decisive here: "The protection of individuals with regard to the processing of personal data is solely governed by [laws including the 1995 *Directive, supra* note 1], which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive".
124. *GDPR*, *supra* note 1, recital 18.
125. Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*, (2010) 00264/10/EN (WP 169) online: <www.pdpjournals.com/docs/88016.pdf>.
126. Found by the Court of Appeal in Northern Ireland to be a data controller under the 1995 *Directive*, *supra* note 1 see *CG v Facebook Ireland Ltd*, [2016] NICA 54.

argues, would not fall foul of the prohibition of obligations to engage in general monitoring in the Directive.[127]

Keller seeks to avoid the conclusion that, since we know from *Google Spain* that search engines are data controllers, platforms like Facebook must be too. She points out that the finding in *Google Spain* was justified by particular reasoning: that the search engine produces a "structured overview" of "vast aspects of [the data subject's] private life … which, without the search engine, could not have been interconnected or could have been only with great difficulty".[128] Keller then argues from this that social media platforms have a *lesser* impact on an individual's privacy, while deleting actual content (instead of merely de-listing it) would have a greater effect on freedom of expression; hence this sufficiently distinguishes social media platforms from search engines.[129] However, these arguments are probably best taken as arguing for a higher burden on those seeking to delete content, rather than merely de-list: she argues that "it should be *harder* to get content removed from a hosting platform, because the balance of rights and interests is different".[130] This is right in part: *in general*, removing content as opposed to simply delisting it when searched under an individual's name will be a greater interference with freedom of expression. Moreover (but also only in general) search engines can have a particularly serious impact on privacy, for the reasons she gives. The key point, however, is that this would not necessarily *always* be the case: as argued below, the extent to which a given piece of online content compromises a person's privacy depends upon a multi-factor assessment, in which perhaps the most important factor is the nature of the information itself.

Two pairs of examples will illustrate the point. Celebrity A is seeking to have Google de-link to some mildly embarrassing gossip-journalism reports about her excessive drinking one evening several years ago. Celebrity B in contrast wants Facebook to remove a post by an estranged friend revealing details of B's past struggles with a serious eating disorder.

127. Erdos, "Intermediary Publishers", *supra* note 6.
128. *Google Spain*, *supra* note 4 at para 80.
129. Keller, "Right Tools", *supra* note 5 at 36.
130. *Ibid* at 43 [emphasis in original].

Here it seems clear that Celebrity B has a far stronger and more serious privacy claim, not least because her case deals with one of the classes of sensitive data.[131] That then demonstrates that claims against hosts *can* raise much more weighty privacy interests than those against search engines.

The second pair of examples considers the freedom of expression side of the balance. Politician C is seeking, shortly before an election, to have Google immediately remove from search returns (pending investigation) links to stories detailing truthful allegations of misconduct during a previous election.[132] Celebrity D is seeking to have topless photographs hacked from her iCloud account removed from a Tumblr site. In this case, although D is seeking to have actual content removed and C merely to have it de-listed, it is clear beyond argument that Google would have a far stronger claim under the freedom of expression derogation than Tumblr: political expression is invariably treated by Strasbourg as the "highest value" speech.[133]

Keller's broad-brush comparison of search engines with social media platforms, therefore, only takes us so far: while the former may *in general* pose a greater threat to privacy but have a weaker free speech claim, it is not hard to generate examples where both propositions are decisively reversed. The conclusion, therefore, seems clear: in each case, a court or regulator would have to treat the status of the data controller (search

131. Namely information relating to health see *GDPR*, *supra* note 1, art 9(1).

132. An example along these lines is actually used by Keller to show the potentially draconian effect of a right to restrict processing under Article 18 (i.e. pulling the item offline), pending investigation as to whether e.g. the data is inaccurate: Keller, "Right Tools", *supra* note 5 at 40.

133. See e.g. *Von Hannover*, *supra* note 25 ("[t]he Court considers that a fundamental distinction needs to be made between reporting facts . . . capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who … does not exercise official functions. While in the former case the press exercises its vital role of 'watchdog' in a democracy by contributing to 'impart[ing] information and ideas on matters of public interest . . . it does not do so in the latter case" at para 63).

engine or host) as but one factor amongst many in weighing the strength of the RTBF claim.

3. Reliance on the Journalism Exemption or Freedom of Expression

The final issue concerns the ability of bodies like Facebook, Twitter and private individuals to claim either the "special purposes" journalism exemption or their own freedom of expression as a defence to RBTF claims. As noted above,[134] the *GDPR* provides in Article 85 for Member States to legislate to provide specific exemptions for freedom of expression and the special purposes. The UK's legislation for this purpose, the *Data Protection Act 2018*, provides a sweeping exemption: the requirements of lawful processing and the other data protection principles, together with all the key rights of the data subject (including Article 17), do not apply where:

> (2) (a) the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material;
>
> (b) the controller reasonably believes that the publication of the material would be in the public interest;
>
> (3) The listed *GDPR* provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes;
>
> (4) In determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information.[135]

This is a very broad exemption,[136] though much will depend on its

134. See above, at 23–24.
135. *2018 Act*, *supra* note 94, schedule 2, paras 26(2)–(4).
136. It is in substance the same (with the addition of "academic purposes") as the exemption provided in the previous *Data Protection Act 1998* (UK), c 29, which implemented the previous Directive, *1995 Directive*, *supra* note 1.

interpretation.[137] The first question is who will fall within it. In *Google Spain*, the CJEU said that "the processing carried out by the operator of a search engine"[138] did not appear to fall within the journalism exemption; Google was not able to rely on it. The English High Court, in the first *Google Spain*-style case heard in the UK,[139] followed this, finding that Google acts:

> for a commercial purpose which, however valuable it may be, is not undertaken for any of the special purposes, or "with a view to" the publication by others of journalistic material. Such processing is undertaken for Google's own purposes which are of a separate and distinct nature.[140]

What then of operators like Facebook and Twitter? Notably in *Google Spain*, the CJEU, in the same paragraph as that cited above, said that "the processing by the publisher of a web page consisting in the publication of information relating to an individual may … be carried out 'solely for journalistic purposes' and thus fall within the journalism exemption".[141] In a more recent decision the CJEU said that activities:

> may be classified as 'journalistic activities' if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit–making purposes.[142]

The importance of intermediaries was recognised by the Advocate General in *Google Spain,* who said that they "act as bridge builders between content providers and internet users … " thus playing a role that "has been considered as crucial for the information society".[143] Also

---

137. Courts are likely to follow the interpretation given to the very similar provision in the 1998 Act: see e.g. *Campbell v MGN*, [2002] EMLR 30 (CA (Eng)) at para 85, confirming that actual publication of newspapers (online and in hard copy) as well as processing *with a view to publication* falls within the exemption.
138. *Google Spain*, *supra* note 4 at para 85.
139. *NT1*, *supra* note 113.
140. *Ibid* at para 100.
141. *Google Spain*, *supra* note 4, at para 85.
142. *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07, [2008] ECR I-09831 at para 61.
143. *Google Spain*, *supra* note 4 at para 36.

of relevance here is Recital 153 of the *GDPR*, which provides:

> In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, *broadly*.[144]

This is in line with the definition of "journalist" given by the Council of Ministers of the Council of Europe, quoted with approval in a recent Strasbourg judgment as being "any natural or legal person who [was] regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication".[145]

All of the above would appear to support the notion that at least *some* content appearing on Facebook, Twitter and the like, could be considered journalism, even where not published by professional journalists. But however broadly and flexibly the notion is interpreted it would seem highly unlikely that it could cover *all* kinds of content: As the High Court in the English *Google*[146] case put it:

> [T]he concept is not so elastic that it can be stretched to embrace every activity that has to do with conveying information or opinions. To label all such activity as "journalism" would be to elide the concept of journalism with that of communication.[147]

Erdos notes that many national DPAs hold that the special purposes derogation "only protects forms of expression undertaken by individuals which are patently akin to that of professional journalism".[148] Even the extensive definition of the Council of Ministers just quoted would confine it to persons *regularly* engaged in "the dissemination of information to the public".[149] This could, for example, include someone who regularly uses Twitter or Facebook to post information about and comment on issues of the day; it would *not* cover someone simply posting pictures of, e.g., a relative's baby. Erdos comments that:

> In referring to special *purposes* rather than special *actors,* [the definition in the

144. *GDPR*, *supra* note 1, recital 153 [emphasis added].
145. *Satakunnan*, *supra* note 60 at para 118.
146. *NT1*, *supra* note 113.
147. *Ibid* at para 98.
148. Erdos, "Domestic", *supra* note 106 at 276.
149. *Satakunnan*, *supra* note 60 at para 118.

> *GDPR*] is not restricted to professional journalists, artists and academic or non–academic writers but rather is in principle open to everyone (a reality given emphasis by the CJEU in *Satamedia*) including private individuals.[150]

And he argues that:

> [T]he *GDPR*'s apparent removal of the [previous] requirement that processing be conceptualised as "solely" for the special expressive purposes as well its general emphasis on construing this clause "broadly" [Recital 153] provides an opportunity to decisively reject … prioritisation of expression by actors with a particular professional status.[151]

He, therefore, concludes that the journalism exemption *should* cover "individuals disseminating a message to the collective public"[152] but that it will probably *not* cover those engaging merely with "self expression" and the "linked general freedom to converse".[153]

If this is right, then courts and regulators will, over time, have to engage in the extremely difficult task of classifying certain content on Twitter and Facebook as posted for journalistic purposes (e.g. comments on politics and current affairs), and some as not (e.g. family pictures). If the *content* is classified as falling within the "journalistic purposes" exemption, there would seem no good reason to hold that the individual poster *can* claim the journalism exemption but that the host (Facebook, Twitter) could not. Even if a court were minded to make this distinction it would make no difference in practice: if only the individual poster was classified as falling within the journalism exemption, a RTBF claim made against Facebook, for example, could be resisted on the basis that the disputed content fell within the purposes of journalism, seen from the perspective of the original poster.

Finally, even where content is *not* considered journalism, a host (or individual user) could still resist an Article 17 request on the basis that "the processing was necessary for exercising the right of freedom of expression"[154] of the original poster. The CJEU has said consistently, as far

150. *Ibid* at 289.
151. *Ibid* at 290.
152. *Ibid*.
153. *Ibid*.
154. *GDPR*, *supra* note 1, art 17(3)(a).

back as the *Lindqvist* case, that both data protection authorities and courts have a duty in certain cases outside of the special purposes exemption to interpret data protection rules with regard for freedom of expression.[155] How far eventual interpretation of the *GDPR* will privilege journalistic purposes over the freedom of expression of ordinary members of the public remains at present a matter of speculation. Much may depend on the particular legislation introduced by national Parliaments,[156] as well as the policies and guidance of national DPAs. What also remains to be seen is how far intermediaries like Facebook and Twitter will go in seeking to defend the freedom of expression of its individual users, given that the original posters of material will not, seemingly be involved at all in decisions on whether to remove the content pursuant to deletion requests. This is something that Keller argues is a major structural problem with

155. *Lindqvist*, *supra* note 20 at para 87.

156. The sweeping exemption granted by the UK's *Data Protection Act 2018*, *supra* note 94, only applies to "special purposes" material, but broader exemptions to protect freedom of expression and information may subsequently be introduced by UK Regulation made under section 16. Section 16(1)(c) gives the Secretary of State power to make regulations for the purposes of the power in Article 85(2) to provide for exemptions or derogations from certain parts of the *GDPR* where necessary to reconcile the protection of personal data with the freedom of expression and information. These will likely be similar to the terms of the previous *Data Protection (Processing of Sensitive Personal Data) Order 2000* (UK), 2000 no 417, which the *2018 Act* revoked (per Schedule 19).

RTBF under European data protection law.[157]

IV. A Possible Role for Article 8 ECHR?

Article 17 is a new and broadly-framed provision and offers little guidance as to its proper interpretation, in particular how the tension it creates with freedom of expression, should be resolved. The Working Party's guidance on *Google Spain* said that, "in determining the balance" between data protection rights and freedom of expression, "the case-law of the European Court on Human Rights is especially relevant".[158] Hence the remainder of this paper will consider how far the Strasbourg's Article 8 privacy jurisprudence may guide interpretation of Article 17, an analysis not yet attempted in the literature. It will do so by elucidating principles from that jurisprudence, and considering whether they are either: (a) applicable to the interpretation of the right to be forgotten; (b) applicable but with modification; or (c) inapplicable.

---

157. Daphne Keller, "The 'Right to Be Forgotten' and National Laws Under the GDPR" *Inforrm* (4 May 2017), online: Inforrm <https://inforrm.org/2017/05/04/the-right-to-be-forgotten-and-national-laws-under-the-gdpr-daphne-keller> (Keller discusses in detail a number of serious issues concerning procedural fairness relating to the handling of RTBF requests under Article 17: she points out that the original speaker who provided the content (e.g. the author of a Tweet) will not be represented during the decision of a host (or search engine) as to whether to remove (or delist) the content, which, she argues, "puts a very heavy thumb on the scales against the [speaker]" at para 15. She also points out that, while data subjects can appeal a refusal to delete to the DPA, and ultimately to the courts, there are "no public correction mechanism for cases where Google actually should de-list *less* [emphasis in original]" (*ibid*, para 18). Finally, in "Right Tools", *supra* note 5, Keller highlights that in most cases, online service providers are not even allowed to tell the accused user that her content has been de-listed or erased. This, she argues, "places the fate of online expression in the hands of accusers and technology companies – neither of whom has sufficient incentive to stand up for the speaker's rights" at para 48).

158. Article 29 Google Spain Guidelines, *supra* note 6 at 14.

A. The General Relevance of Strasbourg Case Law

It is clear beyond argument that Strasbourg jurisprudence will be relevant to the interpretation of the *GDPR*. Article 52(3) of the EU Charter states that when Charter and ECHR rights overlap the ECHR's definition (in effect, Strasbourg's interpretation) of the right should be taken to be the same as that of the corresponding provision within the Charter.[159] In other words Charter rights must be interpreted consistently with ECHR rights that correspond to them and are thus "complementary" to the ECHR rights.[160] Since the right to privacy in Article 8 ECHR corresponds with Article 7 of the EU Charter,[161] Strasbourg jurisprudence is directly relevant to the CJEU and European courts' formulation of Article 17. This is enhanced by the long-standing inter-court comity between the CJEU and Strasbourg. Both courts regularly cite each other's judgments,[162] in many cases the CJEU taking Strasbourg's more experienced lead when adjudicating upon fundamental rights.[163] Over the course of the last decade a strong working relationship between the two courts has been fostered.[164]Further, the "*Bosphorus* presumption", whereby Strasbourg operates a rebuttable presumption that EU law offers

159. EU Charter, *supra* note 21, art 52(3); see Wolfgang Weib, "Human Rights in the EU: Rethinking the Role of the European Convention on Human Rights After Lisbon" (2011) 7:1 European Constitutional Law Review 64 at 64–67.
160. Tommaso Pavone, "The Past and Future Relationship of the European Court of Justice and the European Court of Human Rights: A Functional Analysis" *Social Science Research Network* (28 May 2012) at 13, online: SSRN <https://ssrn.com/abstract=2042867>.
161. EU Charter, *supra* note 21.
162. Noreen O'Meara, "'A More Secure Europe of Rights?' The European Court of Human Rights, the Court of Justice of the European Union and EU Accession to the ECHR" (2011) 12:10 German Law Journal 1813 at 1815.
163. Pavone, *supra* note 160 at 1.
164. O'Meara, *supra* note 162 at 1816. See also Sylvia de Vries, "EU and ECHR: Conflict or Harmony?" (2013) 9:1 Utrecht Law Review 78 at 79 (it has been said that lines are becoming "increasingly blurred" between rights protection afforded between the ECtHR and the CJEU).

rights protection at least equivalent to that of the ECHR, shows the privileged nature of EU law at Strasbourg. Overall, the strong structural relationship between the two courts[165] means that Strasbourg case law is likely to have a significant influence on the interpretation of the EU's new data protection framework.

B. How Strasbourg's Article 8 Jurisprudence Might Apply

Strasbourg has developed the test of whether a claimant had a "reasonable expectation of privacy" ("REP") in order to decide Article 8 claims in a plethora of cases, including *Halford v UK*,[166] *PG & JH v UK*,[167] *Peck v UK*,[168] *Perry v UK*[169] and more recently *Von Hannover v Germany* (*nos 1, 2 & 3*)[170] and *Lillo-Stenberg and Sæther v Norway*.[171] In deciding whether such an expectation arises, Strasbourg uses the factors discussed in Part V below. If a REP is *not* established, the claim fails; if it is, the court proceeds to balance the Article 8 claim against the right to freedom of expression under Article 10; in doing so it will often return to the same

165. Which will be strengthened further once the planned accession of the EU to the ECHR goes ahead, as required by the EC, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, [2007] OJ, C-306/01, art 6(2). The process is currently stalled but see e.g. Christina Eckes, "EU Accession to the ECHR: Between Autonomy and Adaption" (2013) 76:2 Modern Law Review 254; Tobias Lock, "The Future of the European Union's Accession to the European Convention on Human Rights after Opinion 2/13: Is it Still Possible and is it Still Desirable?" (2015) 11:2 European Constitutional Law Review 239.
166. *Halford v United Kingdom*, No 20605/92, [1997] 24 EHRR 523.
167. *PG and JH v United Kingdom*, No 44787/98, [2001] IX ECHR 195 [*PG*].
168. *Peck v United Kingdom*, No 44647/98, [2003] I ECHR 123 [*Peck*].
169. *Perry v United Kingdom*, No 63737/00, [2003] IX ECHR 141 [*Perry*].
170. *Von Hannover*, *supra* note 25; *Von Hannover v Germany (no 2)*, No 40660/08 [2012] I ECHR 399 [*Von Hannover no 2*]; *Von Hannover v Germany (no 3)*, No 8772/10, [2013] V ECHR 264 [*Von Hannover no 3*].
171. *Lillo-Stenberg and Sæther v Norway*, No 13258/09, [2014] ECHR 59 [*Lillo-Stenberg*].

factors in order to consider the *weight* of the privacy claim.[172] There are several different possibilities as to how courts and regulators in Europe might use elements of the REP test to guide their interpretation of Article 17. Different national courts may, at least for some time, produce different interpretations of this relationship, which will remain until authoritative guidance is provided by the CJEU or the new EU Data Protection Board, which will take time. Moreover, given that the *GDPR* specifically allows national legislatures to flesh out aspects of the new regime via national law, there is room for divergent national approaches to flourish permanently, as indeed happened under the previous EU data protection scheme.[173] There is also the intriguing possibility of a clash between the *GDPR* and the European Convention on Human Rights: a claim could be brought to the Strasbourg court that a particular ruling under Article 17 by a national court violates the right to freedom of expression under Article 10.[174]

There are a number of possible approaches that courts and Regulators might take to the relevance of Strasbourg's REP test to Article 17. These include:

1. Determining that the deletion right only applies where the data

172. See H. Tomás Gómez-Arostegui, "Defining 'Private Life' Under Article 8 of the European Convention on Human Rights by Referring to Reasonable Expectations" (2005) 35:2 California Western International Law Journal 153, online: CWILJ <https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?referer=https://www.google.ca/&httpsredir=1&article=1164&context=cwilj>.

173. David Erdos made the first systematic study of national laws implementing Directive 95/46 in terms of the protection they provided for media freedom: see David Erdos, "European Union Data Protection Law and Media Expression: Fundamentally Off Balance" (2016) 65:1 International and Comparative Law Quarterly 139 (he found "a total lack of even minimal harmonisation" (abstract) and, in different member states "outcomes ranging from subjecting the media to entirely inappropriate peremptory rules to completely eliminating the individual's substantive data protection rights when they come into conflict with media expression" at 180).

174. *Satakunnan*, *supra* note 60, concerned such an unsuccessful claim (although not of course in relation to the *GDPR*).

subject has a reasonable expectation of privacy. This would seem an implausibly restrictive interpretation of Article 17, but one that media bodies, including social media companies, may seek to argue before national courts and regulators.

2. Treating the REP test as wholly irrelevant to the right to be forgotten; given the Working Party's clear view of the importance of the Strasbourg jurisprudence[175] this seems unlikely.
3. Using the REP factors *only* in order to reconcile an erasure claim under Article 17 with the freedom of expression exception.[176]
4. Using the test or factors from it to assist in determining whether RTBF would apply only in doubtful or borderline situations, where the deletion request was particularly contentious in some way. In particular, consideration of factors derived from the REP test could help resolve:
    - the scope of the household exemption;[177]
    - in relation to "sensitive" data, whether the individual had deliberately made it public;[178]
    - whether and when hosts should be fixed with liability as data controllers;[179]
    - where the deletion request is made on the basis of the data subject's objection to processing being carried out "for the purposes of legitimate interests pursued by the data controller or a third party", determining which interests can be outweighed by "the interests or fundamental rights and freedoms of the data subject".[180] Factors from the REP test could help determine how strongly those interests are

175. Above, at 39.
176. *GDPR*, *supra* note 1, art 17(3)(a).
177. Discussed above, Part III.C.1.
178. *GDPR*, *supra* note 1, art 9(2)(e) (such a finding could ground an alternative basis for processing other than consent — which may be withdrawn under Article 9).
179. Recalling that in *Google Spain*, *supra* note 4, the CJEU decided that Google should be treated as a data controller partly because of the serious impact that its activities could have on the data subject's privacy.
180. *GDPR*, *supra* note 1, art 6(1)(f).

engaged; and
- the overall balance of a RTBF request with freedom of expression and/or the purposes of journalism.

At this point it will be helpful to give examples of different ways in which personal data may be disseminated online; these may affect the balance between expression and privacy rights and hence how the principles employed by the Strasbourg Court in adjudicating Article 8 claims may apply to the right to erasure.

1. Data Dissemination Scenarios

i. Information concerning a data subject ("A") is uploaded by a third party ("B") without A's consent (the "third party scenario")

Personal data placed online in this manner directly parallels traditional Article 8 claims considered in the Strasbourg case law. Nearly all its privacy jurisprudence concerns non-consensual publication of personal information by a third party, often the press, as in key cases like *Von Hannover*[181] and a more recent decision in which a celebrity couple complained of covert photographs of them published by a Norwegian magazine.[182] In such scenarios, Strasbourg principles pertaining to the weight of the Article 8 claim could be directly "read across" to Article 17 cases. Strasbourg has made clear that the processing of personal data by an external actor that creates a permanent record of an event is a significant consideration in determining whether a REP exists.[183] Indeed Strasbourg has appeared willing to find a breach of Article 8 in relation to personal data merely *stored* by a third party against a subject's wishes.[184] Such storage will often be a significantly less serious breach of privacy than the *dissemination* of personal data online, as would be the case with a claim under Article 17 of the *GDPR*. If European courts take Strasbourg's lead

181. *Von Hannover*, *supra* note 25.
182. *Lillo-Stenberg*, *supra* note 171.
183. *PG*, *supra* note 167.
184. *Amann v Switzerland*, No 27798/95, [2000] II ECHR 245 at para 70.

in this regard this would tend to give Article 17 a wide ambit.[185]

ii. A data subject ("A") made personal data available online; it is reposted without consent to third party sites and A wishes to delete it (the "data leak" scenario)

A crucial factor here will be whether the initial posting was (a) to a restricted forum (e.g. a controlled group of Facebook "friends"); or (b) to the world at large (e.g. on Twitter or to "the public" on Facebook).[186] The Strasbourg case law can be readily used to support an expectation of privacy in scenario (a), *provided* that the data subject could not have reasonably foreseen that the information would be viewed by such a large audience.[187] There are obvious parallels here with *Peck v UK, PG and JH* and *Perry*. In *Peck,* stills of a CCTV recording distributed by the local council of the aftermath of Peck's suicide attempt on a public street (he had attempted to cut his wrists) were broadcast on national television.[188] Strasbourg held that while Peck would have realised that any passers-by in the street at the time could have seen him, he could not reasonably have anticipated that his actions would end up being viewable by a mass audience.[189] Similarly, in both *PG and JH* and *Perry,* Strasbourg found

185. However, the situation would be more difficult were B to publish personal data about A *alongside* information about themselves, e.g. where B uploads a photograph onto a social networking site that shows A and B together. A deletion request would raise a direct conflict between B's autonomy (manifested in their expressive act of posting the photo) and A's autonomy (manifested in their desire to exercise informational control over it); see Geoffrey Gomery, "Whose Autonomy Matters? Reconciling the Competing Claims of Privacy and Freedom of Expression" (2007) 27:3 Legal Studies 404.

186. As already noted, in the former case, at least the poster of the data might well not even be treated as a data controller: above, at 28.

187. In the case of *Peck*, *supra* note 168, the ECtHR stated that Mr Peck, who had attempted to commit suicide on a public street, had a partial expectation of privacy as he could not have reasonably foreseen that the stills of the CCTV footage of the event would be broadcast on television and distributed to other police constabularies.

188. *Peck*, *ibid* at paras 10–15.

189. *Ibid* at para 62; Gómez-Arostegui, *supra* note 172 at 17.

the existence of an REP due to the fact the claimants' data had been processed in more extensive a manner than they could have reasonably foreseen.[190]

However, the Strasbourg REP test does not naturally apply where the data subject had initially uploaded the data to a publically accessible online domain: in such circumstances, Strasbourg would presumably reason that the claimant should have foreseen that in uploading data to a public platform he or she was exposing it to an unknown and hence unlimited amount of users. As such, the claimant would appear to have voluntarily surrendered control over who accesses the data.[191] This reveals a potential tension between the REP test and Article 17. The former focuses upon the degree of publicity that a claimant could have *reasonably foreseen*;[192] Article 17 emphasises the importance of a data subject's ability to rescind their consent to previous publication of private data.[193] As discussed above, this upholds the ability of a subject to regain data privacy lost online (even through their own initial act of publication), rather than focusing only on their expectations at the time of the initial disclosure: in this way Article 17 treats informational self-determination as a *continuing* process.

Despite this difference, can some common ground be found here? In *Pretty v United Kingdom*[194] the Court found that the "notion of personal autonomy is an important principle underlying the interpretation of

190. *PG*, *supra* note 167; *Perry*, *supra* note 169.
191. In all of the following cases the press made personal information known without consent: *Lillo-Stenberg*, *supra* note 171; *Von Hannover*, *supra* note 25; *Von Hannover (no 2)*, *supra* note 170; *Von Hannover (no 3*), *supra* note 170.
192. *Peck*, *supra* note 168; *PG*, *supra* note 167; *Perry*, *supra* note 169.
193. *GDPR*, *supra* note 1, art 17(1)(b).
194. *Pretty v United Kingdom*, No 2346/02, [2002] III ECHR 155.

its guarantees".[195] As discussed above, the right to delete is designed to enhance autonomy in its informational form, by affording individuals greater control over dissemination of their personal data.[196] Given that the application of a conventional REP test would here rob the right to delete of much of its effectiveness, it arguably needs some re-working so as to recognise informational autonomy as a continuing process.[197] Rather than European courts using Strasbourg's REP test to limit the scope of Article 17 right to delete, it might instead be for Strasbourg to reconsider the test in light of Article 17 and the changing nature of privacy in the digital age. The "reasonable expectation" of a user might in appropriate circumstances be said to encompass the ability to rescind a former publication of private data. It should be recalled that if this were accepted, this would only ground a *prima facie* claim for deletion:[198] it would then have to be balanced against freedom of expression under Article 17(3)(a).

195. *Ibid* at para 61; see also Begüm Bulak and Alain Zysset, "'Personal Autonomy' and 'Democratic Society' at the European Court of Human Rights: Friends or Foes?" (2013) 2:1 UCL Journal of Law and Jurisprudence 230. Althaf Marsoof, "Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression" (2011) 19:2 International Journal of Law and Information 110.
196. Reding, *supra* note 27.
197. Above, at 19–20.
198. Which itself would only apply where withdrawal of consent *per se* grounded an Article 7 claim: see above, at 25–26.

V. Factors Going to the Weight of the Article 8 Claim and Their Possible Application to RTBF

A. The Nature of the Information

Strasbourg has previously found that bodily integrity,[199] sexuality,[200] family grief,[201] personal identity[202] and personal information[203] are all aspects of private life under Article 8. In general it has stressed that the more intimate the personal data disclosed, the stronger the claim to privacy will be.[204] An individual's sexual or romantic life is viewed as particularly sensitive and thus an important aspect of their private life.[205] For example, in *Avram v Moldova*, women were secretly filmed by the police frolicking in a sauna with male police officers in a state of partial undress and the footage later passed to local television stations and broadcast. Strasbourg found a breach of Article 8, stressing that an individual's sexual and romantic life should be free from unwanted observation by others.[206]

One area of uncertainty here is the approach taken to "intimate" information. What is considered intimate can vary, depending upon

199. *X and Y v The Netherlands*, No 8978/80, [1985] 8 EHRR 235; see also Lorenc Danaj and Aleks Prifti, "Respect for Privacy from the Strasbourg Perspective" (2012) 2012:5 Academicus: International Scientific Journal 108.
200. *ADT v United Kingdom*, No 35765/97, [2000] IX ECHR 295.
201. *Pannullo and Forte v France*, No 37794/97, [2001] X ECHR 279.
202. *Van Kück v Germany*, No 35968/97, [2003] VII ECHR 1.
203. *Smirnova v Russia*, No 46133/99, [2003] IX ECHR 241.
204. *Von Hannover (no 2)*, *supra* note 170; *Von Hannover (no 3)*, *supra* note 170.
205. See e.g. *Dudgeon v United Kingdom*, No 7525/76, [1981] 4 EHRR 149; and Gómez-Arostegui, *supra* note 172 at 6.
206. *Avram v Moldova*, No 41588/05 (5 July 2011) [*Avram*]; Dirk Voorhoof, "European Court of Human Rights: Avram and other v Moldova" (2012) 1:1 Iris: Legal Observations of the European Audiovisual Observatory 1.

factors such as culture, religion, gender, age and personality type.[207] It is also fact-sensitive: while Strasbourg generally views data concerning an individual's romantic life as peculiarly intimate, in *Lillo-Stenberg v Norway* it held that a wedding was not necessarily a private occasion.[208] As noted above, while Article 17 covers all personal data, the *GDPR* specifies certain categories as particularly sensitive (above, at 22–23). These should, however, be applied with a degree of flexibility, especially when assessing unusual or complex claims. At the national level this may depend upon what specific provision Member States make to allow freedom of expression claims to outweigh the prohibition on processing personal data.[209] Article 17 itself does not distinguish between sensitive and ordinary data, in providing that deletion requests may be refused where necessary "for exercising the right of freedom of expression",[210] but even when engaging in this kind of "pure" balancing act, courts are likely to find that, as the Working Party put it:

> *As a general rule*, sensitive data … has a greater impact on the data subject's private life than 'ordinary' personal data. A good example would be information about a person's health, sexuality or religious beliefs. DPAs are *more likely to intervene* when de-listing requests are refused in respect of search results that reveal such information to the public.[211]

Following this approach, domestic courts may seek to find ways of avoiding automatic consequences that may flow from the classification of data as "sensitive". As Lady Hale said in the leading privacy decision of *Campbell v MGN Ltd*,[212] while medical information relating to health is generally considered obviously private, "[t]he privacy interest in the fact that a public figure has a cold or a broken leg is unlikely to be strong enough to justify restricting the press's freedom to report it. What harm

207. Chris Hunt, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011) 37:1 Queen's Law Journal 167 at 197–200.
208. *Lillo-Stenberg*, *supra* note 170 at para 37.
209. See the example of provisions in the UK's *Data Protection Act 2018, supra* note 156.
210. *GDPR*, *supra* note 1, art 17(3)(a).
211. Article 29 Google Spain Guidelines, *supra* note 6 at 17 [emphasis added].
212. *Campbell*, *supra* note 63.

could it possibly do"?[213] We suggest that courts taking this more flexible, fact-sensitive approach should employ a mixed objective-subjective test, relying upon a mixture of cultural and contextual factors. These could include an examination of what information may normally be considered intimate for someone of the same age or religion, as well as an examination of a subject's personal sensitivities: for example, a person who had had gender reassignment surgery would likely be particularly sensitive about a photograph circulating that showed them as their previous gender.[214]

B. The Form of the Information: Images or Text?

When assessing the strength of Article 8 claims, Strasbourg may take into account the form in which the personal data is disclosed — such as photographs, sound recordings or written text.[215] Thus "privacy may be thought of as being domain specific".[216] Strasbourg has treated privacy rights relating to photographs as particularly significant: as Gomery observes, "it has become plain that the courts treat *images* of a person in a public space differently than they would a *description* of the person in the same place because a photograph may make a data subject clearly 'identifiable'".[217] As Marsoof comments in relation to the English decision in *Douglas v Hello!*:[218]

---

213. *Ibid* at 157.
214. See Hunt, *supra* note 207 at 197–99 arguing that both individual sensitivities and cultural or community norms need to be considered. On privacy as particularly engaging certain types of information bearing on an individual's reputation and therefore their dignity, see generally Ruth Gavison, "Privacy and the Limits of the Law" (1980) 89:3 Yale Law Journal 421 at 457; Robert Post, "Three Concepts of Privacy" (2000) 89:6 Georgetown Law Journal 2087; Robert Gerstein, "Intimacy and Privacy" in Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984) 266 at 270; and David Hughes, "Two Concepts of Privacy" (2015) 31:4 Computer Law & Security Review 527 at 534.
215. See Gomery, *supra* note 185 at 427.
216. Marsoof, *supra* note 195 at 129.
217. Gomery, *supra* note 185 at 427 [emphasis added].
218. [2006] QB 125 (UK) citing *Douglas v Hello!*, *supra* note 77 at para 106.

> the unauthorised publication of photographs has been condemned more forcefully than other forms of privacy leaks. In *Douglas v Hello!* it was observed that "[a] photograph can certainly capture every detail of a momentary event in a way which words cannot, but a photograph can do more than that. A personal photograph can portray, not necessarily accurately, the personality and the mood of the subject of the photograph."[219]

Similarly, in *Von Hannover v Germany (no 2)*,[220] Strasbourg said:

> [A] person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development.[221]

Article 17 does not refer to particular forms of personal data but it appears likely that many individuals will wish to use it to delete online photographs of themselves. Stories abound of online photographs having a subsequent detrimental impact on a person's private life or their career.[222] However other forms of personal data accessible online, including text, also have the potential to be significantly detrimental to a data subject's privacy or reputation, especially if they describe intimate details of, for example, their sex life. Hence courts and regulators should undertake a flexible approach on a case-by-case basis when deciding upon deletion requests. It may often be the case that the *content* of the data and the repercussions of its open accessibility on the data subject are more important than its form.

---

219. Marsoof, *supra* note 195 at 129.
220. *Von Hannover (no 2)*, *supra* note 170.
221. *Ibid* at para 96.
222. Daniel Bean, "11 Brutal Reminders That You Can and Will Get Fired for What You Post on Facebook" *Yahoo* (6 May 2014), online: Yahoo <https://www.yahoo.com/tech/11-brutal-reminders-that-you-can-and-will-get-fired-for-84931050659.html>. See e.g. "Teacher sacked for posting picture of herself holding glass of wine and mug of beer on Facebook" *The Daily Mail Online* (7 February 2011), online: The Daily Mail Online <*www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html*> (schoolteacher Ashley Payne's employment was terminated due to photographs of her on Facebook, showing her drinking alcohol on holiday).

C. Is the Data Subject a Public Figure?

1. The Importance of the "Public Figure" Criterion.

One of the most important factors used by courts and regulators in assessing privacy claims is whether the claimant is a "public figure". In *Google Spain* the CJEU said that the legitimate interest of the public in having information available on social networks "may vary, *in particular, according to the role played by the data subject in public life*".[223] In its commentary on the decision, the Working Party said: "there may be information about public figures that is genuinely private and that should not normally appear in search results, for example information about their health or family members".[224] But it went on:

> [A]s a rule of thumb, if applicants are public figures, and the information in question does not constitute genuinely private information, there will be a stronger argument against de-listing search results relating to them.[225]

The English High Court, when applying *Google Spain* domestically, found this criterion, of "playing a role in public life" to be "broader" than the notion of being a public figure like a politician or sportsperson.[226] But the notion that the Working Party meant to postulate the widest possible approach to the concept of public figure seems doubtful. In particular, their explanation that, "[a] good rule of thumb is to try to decide where the public having access to the particular information … would protect them against improper public or professional conduct",[227]suggests that the fact that a given celebrity was well known to the public would be less important than whether knowing the information in question could protect the public against improper conduct on their part. Given that members of the public are generally not affected by the way in which celebrities behave in their private lives this may suggest a more restricted approach. This is supported further by

223. *Google Spain*, *supra* note 4 at para 81 [emphasis added].
224. Article 29 Google Spain Guidelines, *supra* note 6 at 14.
225. *Ibid* at 14.
226. *NT1*, *supra* note 113 at para 137.
227. Article 29 Google Spain Guidelines, *supra* note 6 at 13.

the Working Party's guidance that:

> [t]here is a basic distinction between a person's private life and their public or professional *persona*. The availability of information in a search result becomes more acceptable the less it reveals about a person's private life.[228]

In sum, the view of the Working Party would seem to point away from the notion that a celebrity, for example, has a reduced expectation of privacy in relation to information concerning core areas of their private life, such as their sex-life, family matters or health, simply by virtue of their fame.

In strong contrast, it appears that Google, when deciding RTBF requests to date, treats "public figure" as meaning simply "someone recognised at national or international level", something it decides simply by "a search of relevant URLs or names".[229] The problem with this is that fame can bear no relationship to importance. An extreme and notorious example is the overweight 16-year-old boy who became known as "Little Fatty": a picture taken of him in the street by chance went viral in Asia with "hit" rates in the tens of millions and eventual coverage in Reuters and the Independent.[230] Clearly this boy would (at least at the time) have fitted Google's definition of a "public figure", since he would be recognised at national *and* international level. But if this is the case then the notion of "public figure" risks becoming completely un-tethered from any links it once had with the notion of a *legitimate* public interest in the persons' doings, as with a politician or public official. It also suggests that one basis for making someone a legitimate target for public attention is simply that in the past they have attracted public attention. Under this approach the media — and indeed ordinary internet users — can reduce a person's expectation of privacy simply by constantly intruding into their privacy. In such circumstances, the very person who needs privacy most — because they are constantly suffering from intrusion — is granted less of it, because of the very attention they are seeking to escape. It may be that this issue will not arise in the large majority of RTBF requests — a

228. *Ibid* [emphasis in original].
229. Brock, *supra* note 16 at 51.
230. Cheung, *supra* note 78.

recent study found that fewer than 5% of delisting requests under *Google Spain* concerned "criminal, politicians or high-profile public figures" [231] — but it is important nonetheless.

2. Strasbourg's Approach to "Public Figures"

The position of the Strasbourg Court in relation to the right to privacy of public figures and celebrities is unclear. The Court has certainly been prepared to find that celebrities and public figures still have rights to privacy: Princess Caroline of Monaco won her first case at Strasbourg despite the finding by the German Constitutional Court that she was a "public figure par excellence"[232] — a finding that led the German courts to hold that she had to tolerate being constantly followed and photographed by paparazzo as she went about her daily life. Strasbourg found that the partial denial by German law of a remedy for such constant intrusive publicity breached Article 8.[233] In *Lillo-Stenberg v Norway,* Strasbourg reiterated that:

> in certain circumstances, even where a person is known to the general public, he or she may rely on a "legitimate expectation" of protection of and respect for his or her private life.[234]

However, Strasbourg does appear to regard a person's public figure status as *reducing* their expectation of privacy. Thus, in *Von Hannover (no 2)* the Grand Chamber said that, "[Princess Caroline] and her partner, who are undeniably very well known, [cannot be viewed as] ordinary private individuals. They must, on the contrary, be regarded as public figures",[235] and hence afforded a somewhat reduced expectation of privacy. It is notable that the reason the Court gave for this finding was not that Princess Caroline is a member of a royal family, or that she performs official functions (she does not) but simply because of her celebrity

231. Brock, *supra* note 16 at 51, citing Google, "Transparency Report: Search Removals Under European Privacy Law" *Google* (2018), online: Google <https://www.google.com/transparencyreport/removals/europeprivacy/>.
232. *Von Hannover*, *supra* note 25 at paras 19–21.
233. *Ibid*.
234. *Lillo-Stenberg*, *supra* note 171 at para 97.
235. *Von Hannover (no 2)*, *supra* note 170 at para 120.

status. Similarly, in *Axel Springer*,[236] the claimant "X" was well known to the public because he played one of the main characters in a popular TV series. The Grand Chamber judgment remarked:

> [T]hat role was, moreover, that of a police superintendent, whose mission was law enforcement and crime prevention. That fact was such as to increase the public's interest in being informed of X's arrest for a criminal offence. Having regard to those factors and to the terms employed by the domestic courts in assessing the degree to which X was known to the public, *the Court considers that he was sufficiently well known to qualify as a public figure.* That consideration thus reinforces the public's interest in being informed of X's arrest and of the criminal proceedings against him.[237]

Furthermore, despite Strasbourg's comments (above) in *Lillo-Stenberg v Norway*, it ultimately found that the couple in question did *not* have a right to privacy in respect of covert photographs taken of their wedding — partly *because* they were celebrities.[238] Such cases appear to show Strasbourg finding public figure status not because of the significance of the claimant's role in public life, but simply on the basis that they are well known to the public. While in the recent Grand Chamber decision in *Couderc and Hachette Filipacchi Associés v. France*[239] the Court appeared in places to row back on this, commenting that "the right of public figures to keep their private life secret is, in principle, wider where they do not hold any official functions",[240] other parts of the judgment deny any such a distinction. Thus the Court immediately added that the principle that politicians "lay themselves open to close scrutiny of their every word and deed by both journalists and the public at large … applies not only to politicians, but to *every person* who is part of the public sphere, whether through their actions or their position".[241] The Court confirmed this approach in a passage that starts by asserting that "exercising a public function or of aspiring to political office" exposes one to greater public

236. *Axel Springer AG v Germany*, No 39954/08, [2012] ECHR 227 [*Axel Springer*].
237. *Ibid* at para 99 [emphasis added].
238. *Lillo-Stenberg*, *supra* note 171.
239. *Couderc and Hachette Filipacchi Associés v France*, No 40454/07, [2015] ECHR 992.
240. *Ibid* at para 119.
241. *Ibid* at para 121 [emphasis added].

scrutiny, but then adds immediately that "certain private actions by public figures cannot be regarded as such, given their potential impact in view of the role played by those persons on the political *or social scene*"[242] — apparently equating the roles of celebrities with politicians and public officials. Strasbourg's notion of "public figure" thus now extends well beyond politicians and others exercising real public power, to encompass those who are simply famous, for whatever reason. In particular, in *Von Hannover (no 2)* and *Axel Springer*, Strasbourg appeared to use "public figure" to mean simply a person in whose doings the public are interested. Used in this way, the public figure doctrine means that the right to privacy is sharply reduced by reference simply to public curiosity; the supposedly sacrosanct distinction between the public interest and what interests the public thus comes close to being (indirectly) collapsed.

3. Conceptual Problems with the "Public Figure" Doctrine

There is, however, a deeper problem with placing reliance on "public figure" status as a reason for reducing a person's *prima facie* expectation of privacy:[243] the concept is inherently analytically imprecise and hence not conducive of clear judicial reasoning. It acts as a relatively crude and generalised proxy for three more precise arguments that by their nature should be fact-sensitive.[244] The first is that aspects of the lives of some well-known people may become so widely publicised that they can no longer meaningfully be considered private. Quite evidently, this is no more than an unhelpful generalization. It clearly will not always be the case and cannot be decided in advance of examining the particular situation before the court. Nevertheless, a softened version of this argument — that being well known to the public per se diminishes one's reasonable

242. *Ibid* at para 120 [emphasis added].
243. The following two paragraphs draw briefly on Phillipson, *supra* note 76.
244. The three arguments correspond to those advanced by Dean Prosser in his classic exposition of the US privacy torts, see William L Prosser, "Privacy" (1960) 48:3 California Law Review 383, discussed and applied in the leading New Zealand decision, *Hoskings v Runting*, [2005] 1 NZLR 1 at para 120.

expectation of privacy — captures exactly Strasbourg's current approach. The second argument is that public figures may reasonably be considered to have consented to publicity about their private life, or "waived" their right to privacy. Such a contention makes two mistakes: first, it *assumes* that all public figures seek publicity voluntarily — which is by no means the case — and second, it draws no distinction between seeking publicity for one's *private* life, and seeking publicity in relation to one's vocation, surely an elementary distinction.

The third argument is that there is a degree of legitimate public interest in aspects of the private lives of public figures, as, for example, in the case of philandering politicians. This, however, is not a reason for reducing the scope of the protection given to public figures, but rather a description of a *countervailing* consideration, to be weighed in the balance against their right to protection for privacy. Even put in those terms it is flawed, because it again amounts to an unhelpful generalization: whether there is a legitimate public interest in the life of the public figure will depend upon the nature of the information in question, their role in public life and whether the information contributes significantly to an important public debate.

Thus far more analytical clarity can be obtained by asking each of the above questions separately and in a highly fact-sensitive way. The first question then turns into a distinct enquiry as to whether the information in question is already in the public domain; in that regard, the Grand Chamber of the Strasbourg Court has recently remarked: "[t]he fact that information is already in the public domain will not necessarily remove the protection of Article 8 of the Convention".[245] The second question is whether the public figure has waived their right to privacy by, for example, deliberately making an aspect of it public — this is considered as a separate factor in the next section. The third question falls outside the scope of this article as it concerns, not the expectation of privacy of the data subject, but the *countervailing* freedom of expression of the publisher of the data. Thus, the better approach would take note of public figure status *only* as a way of deciding whether to move on

245. *Satakunnan*, *supra* note 60 at para 134.

to considering any of the above three distinct issues. This would be a considerably more structured and sophisticated methodology — and one that avoids lumping together in one category politicians and pop stars, central bankers and footballers.

In this area then, it is suggested that reference to Strasbourg's "public figure" jurisprudence when considering RTBF is more likely to confuse than assist. The ability to keep certain aspects of one's life private is an important facet of personal autonomy and human dignity to which all individuals are *prima facie* entitled;[246] the approach suggested above upholds that principle while allowing for sensible exceptions based upon specific consequences that may *flow from* public figure status.

D. Prior Conduct of the Person Concerned as Waiving Their Right to Privacy

The Working Party's guidance on *Google Spain* suggests considering whether the content had been "voluntarily made public" by the data subject or whether at least they might reasonably have foreseen that it "would be made public".[247] Strasbourg has looked more broadly at the "prior conduct" of an individual in terms of either shunning or soliciting publicity when evaluating the strength of Article 8 claims.[248] In terms of the former there is some evidence of Strasbourg treating an individual's previous attempts to *shield* themselves from intrusion as strengthening their Article 8 claim. In *Von Hannover v Germany (no 3)*,[249] the Court acknowledged Princess Caroline's efforts to keep her private life out of the press as a relevant factor (although on the facts sufficiently considered

246. See e.g. *Campbell*, *supra* note 63, upholding in part the privacy claim of the supermodel Naomi Campbell; Gavin Phillipson, "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act" (2003) 66:5 Modern Law Review 726; Gewirtz, *supra* note 58 at 181–82.
247. Article 29 Google Spain Guidelines, *supra* note 6 at 19.
248. *Lillo-Stenberg*, *supra* note 171; *Von Hannover (no 2)*, *supra* note 170; *Von Hannover*, *supra* note 25.
249. *Von Hannover (no 3)*, *supra* note 170.

by the German courts).[250] Similarly, in the first *Von Hannover* case, an important factor was that Princess Caroline had made considerable efforts to shield herself from the public eye.[251] In the case of an ordinary person, the element of constant media interest would of course be absent; however the basic factor of the individual's evidenced desire for a degree of privacy could be read across to an Article 17 claim in our "data leak" scenario: where the initial upload was to a restricted website (for example, viewable only to a small group of "friends" on Facebook), this "prior conduct" could be argued to evince a desire for a degree of privacy in respect of the data, which should lend weight to a deletion request.

The other side of the coin is situations in which an individual has appeared previously to *court* publicity for their private life, a situation which many courts find counts *against* an expectation of privacy.[252] In *Axel Springer* the Strasbourg court found that:

> [t]he conduct of the person concerned prior to publication of the report or the fact that the photo and the related information have already appeared in an earlier publication are also factors to be taken into consideration … However, the mere fact of having cooperated with the press on previous occasions cannot serve as an argument for depriving the party concerned of all protection against publication of the report or photo at issue.[253]

The Court's statement that previous conduct of an individual amounting to solicitation of the press would not deprive a data subject of *all* privacy rights implies that such conduct would act only to *partially* reduce an expectation of privacy. As one of us has previously noted, this statement "is of little comfort to privacy advocates" since all it does is rule out the

---

250. *Ibid* at para 55.

251. *Von Hannover*, *supra* note 25 at paras 68, 74 (the Court noted that, of the complained-of photos, one showed Caroline dining in a secluded place (a corner of a restaurant) and another her relaxing within a private members' club).

252. *Theakston v MGN Limited*, [2002] EWHC 137 (QB) (Ouseley J said that since Theakston, a TV presenter, "has courted publicity … and not complained at it when, hitherto, it has been very largely favourable to him … he cannot complain if publicity given to his sexual activities is less favourable in this case" at para 68).

253. *Axel Springer*, *supra* note 236 at para 92 [emphasis added].

extreme (and implausible) "blanket" version of waiver, in which any prior disclosures to the press negate all protection for private life.[254] Moreover, Strasbourg went on to find that as the claimant, a television actor, had previously given interviews and in doing so revealed certain details about his personal life, his reasonable expectation of privacy (and in turn the strength of a claim he could bring under Article 8) had been reduced:

> In the Court's view, he had therefore actively sought the limelight, so that, having regard to the degree to which he was known to the public, his "legitimate expectation" that his private life would be effectively protected was henceforth reduced.[255]

Notably the judgement did not explain why the claimant's previous choice to reveal certain select details about his personal life led to his reasonable expectation of privacy being reduced with respect to other personal data which he had not voluntarily disclosed.[256]

Under this approach it would appear that a data subject who had initially uploaded personal information to an openly accessible platform online and subsequently wished to remove it (perhaps after it was been posted to third party sites) might be treated as having partially waived their right to privacy. The case would also depend on whether the sole ground that the defendant had to justify processing was consent. Where this is the case, a deletion request can be based simply on revocation of consent.[257] How this will be considered where the initial consent was to what we might term "fully public" processing — that is, publication "to the world" on a public website, remains unclear. The circumstances of the original uploading could be considered in the overall balance with freedom of expression. In such circumstances, courts and regulators could consider, for example, whether the information had been put online when the data subject was significantly younger[258] or at a different

254. Phillipson, *supra* note 76 at 151.
255. *Axel Springer*, *supra* note 236 at para 101 [emphasis added].
256. Phillipson, *supra* note 76 at 150–51.
257. *GDPR*, *supra* note 1, art 17(1)(b); see above, at 25–26.
258. The *GDPR* expressly contemplates the special importance of being able to delete information placed online when the data subject was a child: see *GDPR*, *supra* note 1, recital 38, above at 25–26.

stage of their life in terms of personal life or career. It could be asked whether the data subject now has particularly pressing reasons for wanting to delete the information, as where a graduate was seeking to remove pictures of themselves behaving raucously at university parties because they were now seeking professional employment.[259] At worst, the Strasbourg "waiver" approach could be read across even to a data subject seeking the deletion of personal information published by a third party; if so, the claimant could have their privacy claim deemed weaker by virtue of *previously* having voluntarily disclosed different personal information online.

However this notion that a voluntary disclosure of private information prevents an individual from being able to complain about an involuntary disclosure is *wholly incompatible* with the core value of the individual's right to control over the release of personal information.[260] All of us exercise this right to selective disclosure in our social lives: we may tell one friend an intimate secret and not another; at times be open, at others more reticent. But someone who is shown a friend's personal letter on one occasion does not assume that they have thereby acquired the right to read, uninvited, all other such letters. In other words, to suggest that public figures should be treated as barred from complaining about publicity that is unwanted and intrusive *now*, because they had *previously* sought it, would deny them the very *control* over personal information that is inherent in the notion of personal autonomy: previous disclosures should be treated not as an *abandonment* of the right to privacy, but an *exercise* of it.[261] As suggested above, the advent of a substantive RTBF is a chance to re-conceptualise the notion of control over personal information as a continuing rather than a one-off event. Here it is to be

259. See e.g. Alan Henry, "How You're Unknowingly Embarrassing Yourself Online (and How to Stop)" *LifeHacker* (5 October 2013), online: Lifehacker <lifehacker.com/how-youre-embarrassing-yourself-online-without-knowing-495859415>; Solove, "Speech, Privacy", *supra* note 37 at 17.

260. Phillipson, *supra* note 76 at 150 (we draw briefly on this work in the paragraph that follows).

261. See e.g. Nissenbaum, *supra* note 58; Reiman, *supra* note 72.

hoped that the RTBF will influence Strasbourg, rather than the other way around.

E. Circumstances in Which the Information Was Obtained

In *Lillo-Stenberg v Norway*, the Court emphasised the importance of considering the way in which intrusive photographs were captured, commenting, "the situation would have been different if the photographs had been of events taking place in a closed area, where the subjects had reason to believe that they were unobserved".[262] Thus a claimant's lack of knowledge that photographs may be taken appears to be a factor going to the weight of an Article 8 claim.[263] In the first *Von Hannover* case, the Court observed that one particular, rather undignified, image of the Princess falling over at a private beach club was "taken secretly at a distance of several hundred metres, probably from a neighbouring house, whereas journalists' and photographers' access to the club was strictly regulated".[264] The Court also considered the *frequency* with which photographs were being taken and published, noting that "photos appearing in the tabloid press are often taken in a climate of *continual harassment* which induces in the person concerned a very strong sense of intrusion into their private life or even of persecution".[265]

This factor is easily read across to our "third party scenario", since it is in essence much the same as the large number of cases Strasbourg has considered in which the personal data is initially gathered by a third party (the press) and then disseminated to a mass audience. The fact that the individual had made no disclosure of the data at all would surely add strength to their Article 17 claim. In the "data leak" scenario, where the initial upload was given only restricted access e.g. to Facebook "friends", and the leak to public platforms occurred without notice or consent, it would be easier to draw parallels with the notion of surreptitious

262. *Lillo-Stenberg*, *supra* note 171 at para 39.
263. *Von Hannover*, *supra* note 25 at para 68.
264. *Ibid* at para 68.
265. *Ibid* at para 59 [emphasis added].

gathering, thus strengthening the privacy side of the scales. Here an analogy could be drawn with cases like *Peck* and *Von Hannover*: just as individuals appearing in public places accept that they will be subject to casual observations by passers-by, but do not accept the risk of this being converted, by press coverage into essentially mass-observation, so those uploading pictures to be seen only by "friends" would not anticipate the far greater coverage that would result if the information leaks to publically-available sites.

As noted above, this argument becomes harder where the initial upload was to a publically accessible website: it could then be argued that the data subject should have foreseen subsequent greater publicity, though this might depend on the scale and intrusiveness of that publicity. If the further dissemination was of such a scale or nature as to amount to harassment, parallels could be drawn to the circumstances surrounding photographs captured of Princess Caroline in *Von Hannover v Germany*.[266] Finally there is the scenario in which personal information had been uploaded to an openly accessible website but on an anonymous basis, only for the data subject to be later identified against their wishes. Courts and regulators should take a context-sensitive approach here, recognising the key *expressive* value in being able to "share privately".[267]

F. Does the Personal Data Relate to a Public or Private Location?

Several Strasbourg cases focus upon the physical location in which personal data was obtained in deciding whether it warrants protection under Article 8.[268] A claim to privacy in respect of a photograph taken in a public street is less likely to attract Article 8 protection than if the subject of the picture was in a private dwelling.[269] *Lillo-Stenberg v*

266. *Von Hannover*, *supra* note 25.
267. See *The Author of a Blog v Times Newspapers Ltd*, [2009] EWHC 1358 (QB) for a case that failed to recognize the importance of this value; the notion of "sharing privately" comes from Mills, *supra* note 35.
268. *Von Hannover*, *supra* note 25; *Von Hannover (no 2)*, *supra* note 170; *Peck*, *supra* note 168.
269. See e.g. *Lillo-Stenberg*, *supra* note 171.

Norway concerned photos of a wedding of a celebrity couple who had married outdoors on a publically accessible islet.[270] Strasbourg upheld that Icelandic court's judgment that Article 10 should prevail over the couple's Article 8 claim to bar publication of the photos, partly because it was an outdoor wedding taking place in a public place and holiday destination.[271]

However other cases show a more nuanced approach. In *Pfeifer v Austria*[272] Strasbourg said that Article 8 encompasses "a person's physical and psychological integrity".[273] When attempting to define the scope of the right to privacy in *Niemietz v Germany*,[274] the Court said that "it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there entirely the outside world",[275] seemingly advocating a flexible reading of what a private zone could encompass.[276] However, the key case here is the seminal *Von Hannover v Germany*[277] in which the Court stressed "there is … a zone of interaction … with others, even in a public context, which may fall within the scope of 'private life'".[278] The German courts had held that photographs taken in a physically public location of someone they considered a public figure *par excellence* must be tolerated; the only exceptions were images showing Princess Caroline with her children or in a "secluded place", such as a quiet corner of a restaurant. Strasbourg disagreed, finding that this "secluded place" test was unacceptably narrow; the images depicting Princess Caroline in a public place deserved protection under Article 8 as they gave viewers an

---

270. *Ibid* at paras 5–8.
271. *Ibid* at paras 39–44.
272. *Pfeifer v Austria*, No 24733/04, [2011] ECHR 328.
273. *Ibid*; Bulak & Zysset, *supra* note 195 at 234.
274. *Niemietz v Germany*, No 13710/88, [1992] 16 EHRR 97.
275. *Ibid* at para 29.
276. This approach potentially conflicts with the majority's viewpoint in *Campbell*, *supra* note 63, that some information is "obviously private", see Moreham, *supra* note 50 at 646.
277. *Von Hannover*, *supra* note 25.
278. *Ibid* at para 50; *Avram*, *supra* note 206 at para 37; Gomery, *supra* note 185 at 409.

insight into her personality and "psychological integrity".[279]

The above jurisprudence has obvious relevance to RTBF claims and, if followed, should result in courts and regulators resisting crude notions that an event taking place in a public or semi-public environment cannot for that reason be considered worthy of privacy protection.[280]

VI. Conclusion

At the time of writing, Article 17 is only a few days old and its proper interpretation and likely impact remain matters of profound uncertainty. This article has attempted, using Strasbourg's privacy case law as its primary guide, to offer some preliminary answers to the most pressing questions surrounding the application of the newly-formulated right to online expression. The answers it has proposed are necessarily tentative: much of the analysis has involved applying case-law developed in response to very different scenarios from the online deletion right in the *GDPR*. But we hope that our analysis has at least shown that the RTBF has profound implications for how we think about online privacy. It may be that in the end Article 17 influences Strasbourg's case-law as much as the other way around. What *is* certain is that far more work — by regulators, courts and scholars — is needed to fully work out what Article 17 will mean and how it will impact the world of online expression. Most importantly, we do not yet know how significant a contribution it will make to its overall

279. Bryce Clayton Newell, "Public Places, Private Lives: Balancing Privacy and Freedom of Expression in the United Kingdom" (Proceedings of the 77th ASIS&T Annual Meeting, vol 51, at 1–10, 2014) at 6, online: Social Science Research Network <https://ssrn.com/abstract=247909>; Roger Toulson, "Freedom of Expression and Privacy" (2007) 41:2 The Law Teacher 139 at 140.

280. Prosser, *supra* note 244 (noting that "[t]he decisions indicate that anything visible in a public place may be recorded and given circulation by means of a photograph, to the same extent as by a written description, since this amounts to nothing more than giving publicity to what is already public and what any one present would be free to see" at 394). For a forensic critique see E. Paton-Simpson, "Private Circles and Public Squares: Invasion of Privacy by the Publication of 'Private Facts'" (1998) 61:3 Modern Law Review 318, especially 321–326.

goal: the enhancement of our informational autonomy online and with it, the greater freedom to make life choices that might be inhibited by the fear of behaviour being recorded in permanent form online recedes.[281] As Mayer-Schönberger puts it:

> Since the beginning of time, for us humans, forgetting has been the norm and remembering the exception. Because of digital technology and global networks, however, this balance has shifted. Today … forgetting has become the exception, and remembering the default.[282]

We are about to find out how far the right to be forgotten can start to shift this balance back.

281. Westin, *supra* note 58 at 56; Francis Chlapowski, "The Constitutional Protection of Informational Privacy" (1991) 71:1 Boston University Law Review 133; Gerstein, *supra* note 214; Tom Gerety, "Redefining Privacy" (1977) 12:2 Harvard Civil Rights – Civil Liberties Law Review 233 at 281; Ruth Gavison, "Too Early for a Requiem? Warren and Brandeis Were Right on Privacy vs. Free Speech" (1992) 43:3 South Carolina Law Review 437.

282. Mayer-Schönberger, *supra* note 40 at 2.

Equality at Stake: Connecting the Privacy/Vulnerability Cycle to the Debate about Publicly Accessible Online Court Records

Jacquelyn Burkell* & Jane Bailey**

A considerable amount has been written about the privacy implications of publishing court and tribunal records online. In this article the authors examine the linkages between privacy and vulnerability for members of marginalized communities and, drawing on Calo's "vicious cycle" of privacy and vulnerability, suggest that publicly accessible online court records represent an equality issue as well. Drawing on social science research and privacy theory, the authors demonstrate the potentially disproportionate effect of online court records on members of marginalized communities. They then examine Canadian case law, legislation and policy that impose restrictions on public disclosure of information from court proceedings and disclosure of information within court proceedings to highlight a limited pre-existing recognition of the privacy/vulnerability cycle. In conclusion they suggest that removal of personal information from court records made publicly available online would serve to protect both privacy and equality rights.

---

* Associate Professor, University of Western Ontario Faculty of Information and Media Studies.

** Professor, University of Ottawa Faculty of Law (Common Law Section). Thank you to the Social Sciences and Humanities Research Council for funding Towards Cyberjustice: Rethinking Processual Law, a seven-year Major Collaborative Research Initiatives (MCRI) project of which this paper forms a part. Thanks also to Angela Livingstone for her amazing research assistance and support.

I. Introduction
II. Examination of the Privacy/Vulnerability Cycle in the Literature
A. Privacy and Vulnerability
B. Connecting the Privacy/Vulnerability Cycle to Court Records
1. Vulnerable Populations Over-Represented in Court Proceedings
2. Addressing Marginalization in the Courts
3. Records Reveal Stigmatizing Information
III. Recognition of the Privacy/Vulnerability Cycle in Canadian Law
A. Publication Bans and the Privacy/Vulnerability Cycle
B. Case-by-case Privilege and Deemed/Implied Undertakings
C. Children and the Privacy/Vulnerability Cycle
1. Child Welfare and Family Law Proceedings
2. Youth Criminal Justice Act
D. Sexual Assault Complainants and the Privacy/Vulnerability Cycle
1. Prohibitions on Publication of Identifying Information
2. Restrictions on the Use of Complainants' Past Sexual History
E. Other Equality-Seeking Groups and the Privacy/Vulnerability Cycle
F. The Privacy/Vulnerability Cycle and Online Court Records: Commentary and Policy
IV. Conclusion

> [T]he more information you have about a person or group, the greater the potential to take advantage of them. The fewer advantages a person or group already enjoys, the lesser their ability to resist expectations and requirements of turning over information in exchange for support. The result is a vicious cycle which bears great exploration and may militate in favor of stronger privacy protections for the chronically vulnerable.
>
> Ryan Calo[1]

1. Ryan Calo, "Privacy, Vulnerability, and Affordance" (2017) 66:2 DePaul Law Review 591 at 597.

I. Introduction

Court and tribunal records from around the world are increasingly publicly accessible online. These initiatives offer, as we and others have noted, ground-shifting opportunities for improved access to justice and for the transparency of court proceedings; however, they simultaneously raise serious privacy issues for those involved, willingly or unwillingly, in those proceedings.[2] In this article we explore the complex and iterative relationship, characterized in the epigraph by Calo, between publicly accessible, unredacted, online court records and marginalization, vulnerability and inequality. Specifically, we suggest that members of equality-seeking communities stand to be disproportionately negatively affected by online publication of court records incorporating personal information. In this way, online court records constitute not only a privacy problem, but an equality problem as well. This further dimension adds urgency to the need for privacy and equality-respecting approaches to online publication of court and tribunal records.

We advance our argument in Parts II and III. Part II examines literature and social science evidence relating to privacy and vulnerability, suggesting that members of marginalized communities in Canada, including poor and homeless persons, those suffering from mental illness, racialized minorities and Indigenous peoples, will be disproportionately negatively affected by publicly accessible online court records. Drawing on Calo's "vicious cycle" analogy, we offer three reasons in support of this assertion: (i) members of certain marginalized communities are over-represented in many types of court proceedings; (ii) the impacts of marginalization may force members of these communities to engage with the justice system; and (iii) potentially stigmatizing information

2. Jane Bailey & Jacquelyn Burkell, "Revisiting the Open Court Principle in an Era of Online Publication: Questioning Presumptive Public Access to Parties' and Witnesses' Personal Information" (2017) 48:1 Ottawa Law Review 147; Natalie A MacDonnell, "Disability Disclosure in the Digital Age: Why the Human Rights Tribunal of Ontario Should Reform its Approach to Anonymized Decisions" (2016) 25:1 Journal of Law and Social Policy 109; Karen Eltis, *Courts, Litigants and the Digital Age: Law, Ethics and Practice* (Toronto: Irwin Law, 2012) at 5.

about these individuals in court records renders them vulnerable to increased discrimination and other kinds of harms. Part III looks at the degree to which Canadian law has recognized and responded to the privacy/vulnerability cycle in relation to court and tribunal records. After examining court rulings about publication bans and rules relating to disclosure within proceedings, this section specifically examines privacy protections afforded to certain vulnerable groups, including children, sexual assault complainants (who are disproportionately likely to be women) and persons with disabilities, as well as public commentary relating to online publication of court records. Some of these decisions and commentators implicitly or explicitly recognize the privacy/vulnerability cycle that connects a lack of privacy with exposure to inequality and discrimination, thereby offering at least some analysis that can be used to support removing personal information from publicly accessible online court records. The conclusion recommends a response that disrupts the "vicious cycle" without presuming or suggesting that members of equality-seeking communities *must* or *ought* to conceal certain information about themselves.

II. Examination of the Privacy/Vulnerability Cycle in the Literature

Jeffrey Rosen, in *The Unwanted Gaze*, noted that "[t]he ideal of privacy … insists that individuals should be allowed to define themselves, and to decide how much of themselves to reveal or conceal in different situations".[3] Rosen's remarks are echoed in Nissenbaum's concept of information privacy as "contextual integrity".[4] According to Nissenbaum, privacy violations occur when personal information is used in ways that are incompatible with norms of appropriate use and appropriate distribution.[5] The ability to control the use and dissemination of

3. Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage Books, 2000) at 223.
4. Helen Nissenbaum, "Privacy as Contextual Integrity" (2004) 79:1 Washington Law Review 119.
5. *Ibid* at 125.

information about oneself is important. Intimate relationships depend on a delicate interplay between concealment and disclosure.[6] Privacy offers us personal autonomy, and supports important social values including democracy.[7] While it can and has been used to shield abuse of members of equality-seeking groups from public scrutiny and censure,[8] it can also afford members of equality-seeking groups, including women, opportunities for "replenishing solitude and independent decision making," as well as freedom from censure, surveillance and pressures of conformity.[9] Everyone, including members of equality-seeking groups, needs – and deserves – privacy.

A. Privacy and Vulnerability

Nonetheless, there are many cases in which privacy is closely, and negatively, tied to vulnerability and marginalization. Economic marginalization and lack of privacy go hand in hand. Some have argued that privacy is becoming a "luxury good",[10] available primarily to those who can afford to pay to achieve it.[11] This is particularly true online, where 'free' services are in fact purchased with the currency of personal information, and the price of freedom from online surveillance is paid in cash – either by use of services hidden behind "paywalls", or through the purchase of privacy-protecting technologies and software. Those living in

---

6. Sandra Petronio & Irwin Altman, *Boundaries of Privacy: Dialectics of Disclosure* (Albany: State University of New York Press, 2002).
7. Nissenbaum, *supra* note 4 at 128-29.
8. Catharine MacKinnon, *Toward a Feminist Theory of the State* (Massachusetts: Harvard University Press, 1989) at 191.
9. Anita L Allen, "Still Uneasy: Gender and Privacy in Cyberspace" (2000) 52:5 Stanford Law Review 1175 at 1179. See also Patricia J Williams, *The Alchemy of Race and Rights: Diary of a Law Professor* (Cambridge: Harvard University Press, 1991) at 164-65.
10. Julia Angwin, "Has Privacy Become a Luxury Good?" *The New York Times* (3 March 2014), online: NY Times <www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html>.
11. Michael Rosenberg, "The Price of Privacy: How Access to Digital Privacy is Slowly Becoming Divided by Class" (2016) 20:1 UCLA Journal of Law and Technology 1.

poverty can afford neither, and as a result cannot benefit from the privacy protection that these purchases support. In the United States, many have argued that Fourth Amendment protection is reduced for the poor,[12] specifically because they are less able to afford to buy homes.[13] Although the issue has not been widely addressed in Canada, some empirical research suggests that homeless people's contacts with law often involve invasion of their section 8 rights under the *Canadian Charter of Rights and Freedoms*.[14] These individuals are vulnerable to arbitrary search and seizure because they lack a prototypical 'home' within which they would be presumed to have an expectation of privacy. Technological advances in surveillance may further erode the privacy of those living in poverty.[15] GPS tracking technologies, for example, are more easily deployed against the urban poor, since their vehicles are more likely than those of wealthier citizens to be parked in a public location and thus be accessible for the placement of the devices.[16] Poverty, then, leads to conditions in which

12. John Berry, "Nowhere to Hide: How the Judiciary's Acceptance of Warrantless GPS Tracking Eliminates the Practical and Legal Privacy Enjoyed by the Poor" *Social Science Research Network* (2011), online: SSRN <https://ssrn.com/abstract=1949387>; Christopher Slobogin, "The Poverty Exception to the Fourth Amendment" (2003) 55:1 Florida Law Review 391; Kami Chavis Simmons, "Future of the Fourth Amendment: The Problem with Privacy, Poverty and Policing" (2014) 14:2 University of Maryland Law Journal of Race, Religion, Gender & Class 240.
13. See Justin Stec, "Why the Homeless are Denied Personhood Under the Law: Toward Contextualizing the Reasonableness Standard in Search and Seizure Jurisprudence" (2006) 3:2 Rutgers Journal of Law & Urban Policy 321; Mark A Godsey, "Privacy and the Growing Plight of the Homeless: Reconsidering the Values Underlying the Fourth Amendment" (1992) 53:3 Ohio State Law Journal 869.
14. Carol Kauppi & Henri Pallard, "Homeless People and the Police: Unreasonable Searches and Seizures, and Arbitrary Detentions and Arrests" (2009) 1:6 Conference of the International Journal of Arts and Sciences 344, online: Open Access Library <openaccesslibrary.org/images/MAL231_Henri_Pallard.pdf>.
15. Amelia L Diedrich, "Secure in Their Yards? Curtilage, Technology, and the Aggravation of the Poverty Exception to the Fourth Amendment" (2011) 39:1 Hastings Constitutional Law Quarterly 297.
16. Berry, *supra* note 12.

privacy is more difficult to attain, or easier to invade.

The privacy of members of vulnerable communities can be, and is, compromised by surveillance directed toward those communities. Surveillance of welfare recipients has in some cases been justified on the basis that they are receiving assistance from the state,[17] but others have argued that this surveillance most significantly affects single, racialized mothers.[18] In the United States, many jurisdictions require welfare recipients to undergo government mandated drug testing.[19] Techniques of public health screening and surveillance are also selectively directed towards vulnerable members of society. One example is a drug-screening program for pregnant women, enacted by the Medical University of South Carolina in the late 1980's.[20] The program, designed to reduce the impact of prenatal cocaine use on fetuses, was directed specifically toward women who had not obtained prenatal care and those with a previous history of drug or alcohol abuse. If the woman tested positive, the results were turned over to the police, and the woman was threatened with prosecution in order to force her into treatment. A great deal has been written about the legality of the program, along with analyses of the US Supreme Court decision that determined that the testing violated

17. Mike Dee, "Welfare Surveillance, Income Management and New Paternalism in Australia" (2013) 11:3 Surveillance & Society 272; Krystle Maki "Neoliberal Deviants and Surveillance: Welfare Recipients Under the Watchful Eye of Ontario Works" (2011) 9:1/2 Surveillance & Society 47; Paul Henman & Greg Marston, "The Social Division of Welfare Surveillance" (2008) 37:2 Journal of Social Policy 187.
18. John Gilliom, *The Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (Chicago: University of Chicago Press, 2001).
19. Celia Goetzl, "Government Mandated Drug Testing for Welfare Recipients: Special Need or Unconstitutional Condition?" (2013) 15:5 University of Pennsylvania Journal of Constitutional Law 1539.
20. Lawrence O Gostin, "The Rights of Pregnant Women: The Supreme Court and Drug Testing" (2001) 31:5 Hastings Centre Report 8. See also Kristina B Wolff, "Panic in the ER: Maternal Drug Use, the Right to Bodily Integrity, Privacy, and Informed Consent" (2011) 39:5 Politics & Policy 679.

Fourth Amendment rights.[21] For our purposes, however, the fact that this program was ruled unconstitutional is less relevant than the fact that the testing, and the negative effects emanating from it, were highly discriminatory, affecting primarily low-income and racialized women. This is just one of many examples where surveillance is directed at vulnerable populations, with predictable and often negative results.

There exist myriad examples of selective use of privacy-compromising technologies by police against members of marginalized communities. In Canada, DNA technology and "voluntary" DNA collection programs have been deployed in the context of law enforcement initiatives relating to violence against Indigenous women and girls. These include an initiative involving the collection of DNA and other personal information from women (often Indigenous women) engaged in what have been termed "vulnerable lifestyles", as well as an initiative involving the collection of DNA from men living in a remote First Nations community that was the site of the violent death of a young girl.[22] Police stops of racialized youth, particularly young men, are so common that the phrase "driving while black" has become part of the public lexicon.[23] For example, recent data from Ottawa indicate that police there are disproportionately likely to target Middle Eastern and black drivers for "random" traffic stops.[24]

---

21. See *e.g.* Andrew E Taslitz, "A Feminist Fourth Amendment? Consent, Care, Privacy, and Social Meaning in *Ferguson v. City of Charleston*" (2002) 9:1 Duke Journal of Gender Law & Policy 1.
22. Jane Bailey & Sara Shayan, "Missing and Murdered Indigenous Women Crisis: Technological Dimensions" (2016) 28:2 Canadian Journal of Women and the Law 321.
23. David A Harris, "The Stories, the Statistics, and the Law: Why 'Driving While Black' Matters" (1999) 84:2 Minnesota Law Review 265.
24. Ontario Human Rights Commission, *OHRC Response to the Race Data and Traffic Stops in Ottawa Report*, (Ontario: OHRC, 18 November 2016), online: OHRC <www.ohrc.on.ca/en/ohrc-response-race-data-and-traffic-stops-ottawa-report>; Lorne Foster, Les Jacobs & Bobby Siu, "Race Data and Traffic Stops in Ottawa, 2013-2015: A Report on Ottawa and the Police Districts" (Ottawa Police Services Board and Ottawa Police Service, October 2016) at 3 online: Ottawa Police <https://www.ottawapolice.ca/en/about-us/resources/.TSRDCP_York_Research_Report.pdf>.

Not only do conditions of marginalization – *e.g.* poverty – make people more vulnerable to privacy intrusions; privacy intrusions have the potential to increase the effects of marginalization. As Kimberly Bailey points out, "because privacy makes an individual less vulnerable to oppressive state social control, the deprivation of privacy can be an important aspect of one's subordination".[25] Michele Estrin Gilman makes a similar point about the impact of privacy intrusions (in this case, on the poor), suggesting that "the poor as a group suffer extreme privacy violations, which in turn pose a barrier to self-sufficiency and democratic participation".[26]

Privacy violations can increase marginalization by signaling that the victims lack social standing or somehow *deserve* the intrusion.[27] The widespread practice of "carding", for example, signals to others that those stopped by police might be dangerous, thus potentially altering attitudes and behavior toward them. Increased surveillance – and the lack of privacy that it entails – increases the risk that *some* wrongdoing will be identified. Paul Henman and Greg Marston, for example, discuss the "risk logic" of compliance activities in the Australian social security system.[28] That system uses statistical profiling to identify clients who share characteristics with those who have in the past "been incorrectly paid" (read: committed welfare fraud). Even though individuals identified as having these characteristics may never themselves have "been incorrectly paid," they are subjected, by virtue of their statistical resemblance to the group who *have,* to increased surveillance – which, by its very nature, increases the likelihood that "incorrect payments" will be identified. The system is a self-reinforcing feedback loop that creates an underclass within the larger

25. Kimberly D Bailey, "Watching Me: The War on Crime, Privacy, and the State" (2014) 47:5 UC Davis Law Review 1539 at 1542.
26. Michele Estrin Gilman, "The Class Differential in Privacy Law" (2012) 77:4 Brooklyn Law Review 1389 at 1395.
27. See Craig Konnoth, "An Expressive Theory of Privacy Intrusions" (2017) 102:4 Iowa Law Review 1533 for a discussion of this point. See also Julilly Kohler-Hausmann, "'The Crime of Survival': Fraud Prosecutions, Community Surveillance and the Original 'Welfare Queen'" (2007) 41:2 Journal of Social History 329.
28. Henman & Marston, *supra* note 17 at 200.

(and vulnerable) group of those receiving social benefits from the state. Jessica Roberts explicitly ties a lack of privacy to discrimination, noting that "[u]nlawful discrimination … frequently requires discriminators to have knowledge about protected status".[29] Roberts' analysis suggests that privacy may be important to prevent discrimination.[30] While we do not believe that privacy protections could or should supplant equality-based anti-discrimination measures and education, in a context in which identifiability as a member of particular marginalized communities is the basis for discrimination, it seems logical to suggest that privacy intrusions have the potential to foster discriminatory practices and thus privacy protection could help to reduce discrimination.

B. Connecting the Privacy/Vulnerability Cycle to Court Records

Calo identifies the relationship between privacy and vulnerability as a "circle" or "cycle": "the more vulnerable a person is, the less privacy they tend to enjoy; meanwhile, a lack of privacy opens the door to greater vulnerability and exploitation".[31] In the remainder of this paper, we explore one version of this "vicious cycle", examining the links between privacy, vulnerability, and the open (and increasingly online) publication of court records.

We have argued elsewhere that although public access to court records is consistent with the open court principle, which supports transparency of court proceedings, public access to unredacted court records, particularly if placed online, presents significant and unwarranted privacy risks to those involved in court processes.[32] These files often contain information that is deeply personal and potentially very sensitive, including identifying information, financial information, details about relationships, and

29. Jessica L Roberts, "Protecting Privacy to Prevent Discrimination" (2015) 56:6 William and Mary Law Review 2097 at 2097.
30. *Ibid* at 2101.
31. Calo, *supra* note 1 at 591.
32. Bailey & Burkell, *supra* note 2.

details about health status.[33] The release of this information exposes litigants, witnesses and others identified in the court processes to a variety of risks, including identity theft and extortion.[34] Those identified in the records can suffer dignity harms when highly personal information such as the details of a marital breakdown become publicly available.[35] When the information in the records includes details about protected status, there is also the risk of discrimination.[36]

Members of marginalized communities stand to suffer the most significant privacy harms from open court records that include names along with a vast array of other identifying, and often highly personal, information. In the following section, we identify three bases for this argument: first, members of marginalized communities are over-represented in many kinds of court proceedings; second, in order to contest (and potentially redress) the impact of marginalization, members of these communities are forced to engage with the justice system; third, the potentially stigmatizing information that is revealed about these individuals in court records leaves them vulnerable to increased discrimination and other harms.

1. Vulnerable Populations Over-Represented in Court Proceedings

Members of equality-seeking groups bear a larger privacy burden related to open court records to the extent that they are over-represented among those identified in those court records. Few statistics exist to document the demographic characteristics of individuals involved in the court system as defendants or parties, and even less evidence exists with respect

33. Peter A Winn, "Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information" (2004) 79:1 Washington Law Review 307; Sujoy Chatterjee, "Balancing Privacy and the Open Court Principle in Family Law: Does De-Identifying Case Law Protect Anonymity?" (2014) 23:1 Dalhousie Journal of Legal Studies 9; Bailey & Burkell, *ibid* at 148.
34. Bailey & Burkell, *ibid* at 175.
35. Chatterjee, *supra* note 33 at 97.
36. Roberts, *supra* note 29 at 2101.

to witnesses and others (*e.g.* children in family court cases) who are discussed in court proceedings. Nonetheless, analysis of involvement with the criminal justice system and examination of factors related to child protection issues and the incidence of justiciable problems strongly suggests that members of equality-seeking groups are likely to be over-represented in court records.

Involvement with the criminal justice system is correlated with a range of overlapping marginalizing conditions. There is widespread recognition of the negative correlation between socioeconomic status and involvement with the criminal justice system: those lower on the socioeconomic scale are over-represented in the system.[37] The limited body of research on the relationship between homelessness and the criminal justice system suggests that homeless individuals, including street-involved youth, are at an increased risk of involvement with the criminal justice system.[38] A 2002 report on homeless individuals in Calgary, for example, indicated that over three-quarters had at some point in their lives been incarcerated,[39] and homelessness and incarceration have a reciprocal relationship: homelessness increases the risk of incarceration,

37. Ruth R Kipping et al, "Multiple Risk Behaviour in Adolescence and Socio-Economic Status: Findings from a UK Birth Cohort" (2015) 25:1 European Journal of Public Health 44.
38. Sylvia Novac et al, "Justice and Injustice: Homelessness, Crime, Victimization, and the Criminal Justice System" (2006) Centre for Urban and Community Studies, online: University of Toronto <www.urbancentre.utoronto.ca/pdfs/researchprojects/Novacet-al-207-JusticeHomeless2006.pdf>; Employment and Social Development Canada, "Mental Health Courts: Processes, Outcomes and Impact on Homelessness" by Sue-Ann MacDonald et al, (Montreal: Université de Montreal, May 2014), online: Canadian Observatory on Homelessness <www.homelesshub.ca/sites/default/files/ HKDFinalReport_2014.pdf >.
39. Helen Gardiner & Kathleen Cairns, "2002 Calgary Homelessness Study" *Calgary Homeless Foundation* (October 2002) at 46, online: CHF <http://homelesshub.ca/sites/default/files/Calgary%20 Homelessness%20 Study%202002.pdf>.

which is in turn associated with higher rates of homelessness.[40] Among women who have been incarcerated, poverty is strongly associated with recidivism, and thus involvement anew in criminal justice proceedings.[41]

In the United States, race is strongly associated with arrest history, particularly for males, with black males having a much higher probability of arrest record than any other group.[42] Canadian data show a similar picture, indicating that black inmates are over-represented in the incarcerated population.[43] In Canada, a similar situation exists with respect to the Indigenous population. Indigenous people make up 4.3% of the general population, but 24.6% of the inmate population.[44] Indigenous *women* are even more over-represented, comprising 35% of federal prison inmates, and are Canada's fastest growing prison population.[45] Gender non-conforming youth, and particularly youth identifying as transgender, are more likely to be involved with the youth

40. "Criminal Justice, Homelessness & Health" *National Healthcare for the Homeless Council* (2011) online: NHCHC <www.nhchc.org/wp-content/uploads/2011/09/CriminalJustice2011_final.pdf>.
41. Kristy Holtfreter, Michael D Reisig & Merry Morash, "Poverty, State Capital, and Recidivism Among Women Offenders" (2004) 3:2 Criminology & Public Policy 185.
42. Robert Brame et al, "Demographic Patterns of Cumulative Arrest Prevalence by Ages 18 and 23" (2014) 60:3 Crime & Delinquency 471.
43. As of 2015, the "federal incarceration rate for Blacks [was] three times their representation in Canadian society". See Canada, Office of the Correctional Investigator, *Annual Report of the Office of the Correctional Investigator 2014-2015*, by Howard Sapers (Ottawa: OCI, 26 June, 2015), online: OCI <www.oci-bec.gc.ca/cnt/rpt/annrpt/annrpt20142015-eng.aspx>.
44. *Ibid*.
45. *Ibid*.

criminal justice system.[46]

In a 2012 report, the Mental Health Commission of Canada[47] noted the over-representation in the criminal justice system of those living with mental health issues; this issue may be particularly acute among youth.[48] This over-representation, also observed in the United States, has been attributed in large part to deinstitutionalization.[49] Although there is growing recognition that mental illness is unfairly criminalized in Canada,[50] programs designed to divert those with mental illness before they are charged (police-based diversion programs) are of limited effectiveness given the lack of treatment options for those living with mental illness.[51] Persons with intellectual disabilities are also over-represented in the criminal justice system,[52] in part as a result of their lack of understanding

46. Angela Irvine, "We've Had Three of Them: Addressing the Invisibility of Lesbian, Gay, Bisexual, and Gender Nonconforming Youths in the Juvenile Justice System" (2010) 19:3 Columbia Journal of Gender and Law 675; Jerome Hunt & Aisha C Moodie-Mills, "The Unfair Criminalization of Gay and Transgender Youth: An Overview of the Experiences of LGBT Youth in the Juvenile Justice System" *Center for American Progress* (29 June 2012), online: Center for American Progress <https://www.americanprogress.org/issues/lgbt/reports/2012/06/29/11730/the-unfair-criminalization-of-gay-and-transgender-youth/>.
47. Mental Health Commission of Canada, *Changing Directions, Changing Lives: The Mental Health Strategy for Canada* (Calgary: MHCC, 2012), online: MHCC <strategy.mentalhealthcommission.ca/pdf/strategy-images-en.pdf>.
48. Michele Peterson-Badali et al, "Mental Health in the Context of Canada's Youth Justice System" (2015) 19:1 Canadian Criminal Law Review 5.
49. Gary Chaimowitz, "The Criminalization of People with Mental Illness" (2012) 57:2 Canadian Journal of Psychiatry 1.
50. *Ibid* at 5.
51. *Ibid*.
52. Jessica Jones, "Persons with Intellectual Disabilities in the Criminal Justice System" (2007) 51:6 International Journal of Offender Therapy and Comparative Criminology 723.

of court processes and their rights within those processes.[53] Within the criminal justice system, defendants with mental health issues can in some circumstances be diverted to special mental health courts,[54] "designed to deal with accused persons who are experiencing mental health difficulties with understanding and sensitivity".[55] Defendants must meet strict criteria before diversion to these special courts: primary among these is the condition that the individual must be diagnosed with a mental disorder.[56] The mere fact of diversion to these courts, therefore, reveals meaningful and likely stigmatizing information about the individual whose case is diverted. Despite this, mental health court records[57] and the results of appeals from those courts are *not* routinely anonymized across Canada.[58]

Over-representation of marginalized populations is not limited to

53. Susan C Hayes, "Prevalence of Intellectual Disability in Local Courts" (1997) 22:2 Journal of Intellectual & Developmental Disability 71. See also Voula Marions et al, "Persons with Intellectual Disabilities and the Criminal Justice System: A View from Criminal Justice Professionals in Ontario" (2017) 64:1 Criminal Law Quarterly 83.
54. Steven K Erickson, Amy Campbell & Steven J Lamberti, "Variations in Mental Health Courts: Challenges, Opportunities, and a Call for Action" (2006) 42:4 Community Mental Health Journal 335.
55. "Mental Health Court" *Legal Aid Ontario*, online: Legal Aid Ontario <lawfacts.ca/mental-health/court>.
56. See for example the eligibility for Mental Health Court in Nova Scotia: See, "Nova Scotia Mental Health Court Program" *Courts of Nova Scotia*, online: Courts of Nova Scotia <www.courts.ns.ca/Provincial_Court/NSPC_mental_health_program.htm>.
57. For example, hearings in and records relating to Vancouver's Downtown Community Court are public.
58. See, for example: *R v E*, 2012 NLCA 26. We have chosen to anonymize citations that raise the very privacy and equality concerns discussed in this article.

the criminal justice system. In Canada[59] and elsewhere,[60] Indigenous children, and thus their parents, are at increased risk for involvement in the child welfare system. Similarly, parents with intellectual disabilities constitute a higher proportion of child protection cases than would be expected given the prevalence of intellectual disabilities in the general population.[61] One study of the BC child protection system documented a litany of intersecting challenges facing those (mostly women) involved in that system, including domestic violence, mental health issues, poverty, and addiction issues; that study also noted the over-representation of Indigenous mothers in the child protection cases they reviewed.[62] Although child welfare system proceedings are protected from public access, in many of these cases there are concurrent criminal and/or family proceedings that do *not* automatically receive such protection;[63] thus, the greater involvement of individuals from equality-seeking groups in these matters is likely to be associated with involvement in other justice system proceedings that *do* present privacy risks.

Members of vulnerable groups including Indigenous peoples, immigrants, those receiving social assistance, members of ethnic minorities, and those living with disabilities are more likely to experience justiciable problems such as personal injury, family breakdown, or issues

---

59. Nico Trocmé, Della Knoke & Cindy Blackstock, "Pathways to the Overrepresentation of Aboriginal Children in Canada's Child Welfare System" (2004) 78:4 Social Service Review 577.
60. Clare Tilbury, "The Over-Representation of Indigenous Children in the Australian Child Welfare System" (2009) 18:1 International Journal of Social Welfare 57.
61. Stephon Proctor & Sandra Azar, "The Effect of Parental Intellectual Disability Status on Child Protection Service Worker Decision Making" (2013) 57:12 Journal of Intellectual Disability Research 1104.
62. Judith Mosoff et al, "Intersecting Challenges: Mothers and Child Protection Law in BC" (2017) 50:2 UBC Law Review 435.
63. Canada, Department of Justice, "Concurrent Legal Proceedings in Cases of Family Violence: The Child Protection Perspective" by Nicholas Bala & Kate Kehoe (Ottawa: DOJ, 2013), online: DOJ <www.justice.gc.ca/eng/rp-pr/fl-lf/famil/fv-vf/child_protection.pdf>.

with assistance programs.[64] These problems, moreover, tend to occur in clusters: for example, legal problems related to separation are often accompanied by problems with domestic violence, and other issues related to family breakdown such as custody and access.[65] Similarly, individuals living with disabilities are not only more likely to experience these types of problems; they also experience *more* such problems.[66] To the extent that members of marginalized groups recognize their problems as *legal* problems or are involved with others who do, they may be more likely to be involved, and involved more intensely, with the civil justice system.

Many of these risk factors intersect in the lives of affected individuals, with a compounding impact on the likelihood that the individual will be involved with the court system. Mental health issues and drug use are elevated among the homeless population.[67] People with mental health challenges often live in poverty, while mentally ill and homeless adults are more likely to be involved in the criminal justice system if they also experience substance misuse and previous victimization.[68] Indigenous peoples are more likely than the general population to live in conditions of homelessness.[69]

---

64. Canada, Department of Justice, "The Legal Problems of Everyday Life: The Nature, Extent and Consequences of Justiciable Problems Experienced by Canadians", by Ab Currie (Ottawa: DOJ, 2007), online: DOJ <www.justice.gc.ca/eng/rp-pr/csj-sjc/jsp-sjp/rr07_la1-rr07_aj1/rr07_la1.pdf>; Alexy Buck, Nigel Balmer & Pascoe Pleasence, "Social Exclusion and Civil Law: Experience of Civil Justice Problems Among Vulnerable Groups" (2005) 39:3 Social Policy & Administration 302.
65. Pascoe Pleasence et al, "Multiple Justiciable Problems: Common Clusters and Their Social and Demographic Indicators" (2004) 1:2 Journal of Empirical Legal Studies 301.
66. A O'Grady et al, "Disability, Social Exclusion, and the Consequential Experience of Justiciable Problems" (2004) 19:3 Disability & Society 259.
67. Katherine H Shelton et al, "Risk Factors for Homelessness: Evidence from a Population-Based Study" (2009) 60:4 Psychiatric Services 465.
68. Laurence Roy et al, "Profiles of Criminal Justice System Involvement of Mentally Ill Homeless Adults" (2016) 45:1 International Journal of Law and Psychiatry 75 at 79.
69. Novac et al, *supra* note 38.

An exhaustive review of the relationship between vulnerability and justice system involvement is beyond the scope of this paper, but the pattern is clear: people who are socially marginalized are more likely to be involved with the justice system (or at least with certain aspects of it). Those individuals involved in the system are also vulnerable to the privacy harms that result from being identified in court records. Those harms, therefore, are differentially affecting specific groups – the socially marginalized who are, by virtue of a wide range of factors, more likely to be in the courts.

2. Addressing Marginalization in the Courts

Marginalized individuals suffer harms related to their marginalized status – and one way to address these harms is to seek relief in the courts or through administrative tribunals. These situations constitute a kind of double jeopardy or recursive effect: vulnerability leads to involvement with the justice system, which leads to loss of privacy, including privacy with respect to vulnerable status, which in turn can lead to increased discrimination.

Homeless individuals, for example, have been involved in court proceedings that test their right to erect shelters in public parks[70] or on city property,[71] with the result that their names are made public along with details of their homeless status. 'Safe Streets' legislation, passed in Ontario[72] and in British Columbia,[73] prohibits "aggressive solicitation of persons in public places", allowing police to issue tickets for panhandling. Given that the individuals so charged are typically living in conditions of poverty, it is not surprising that the tickets often go unpaid. At least one individual has been taken to court over unpaid fines.[74] This individual opted to participate in press interviews about the case, and thus forewent his privacy with respect to the court proceeding and personal information

70. *Abbotsford (City) v S*, 2015 BCSC 1909.
71. *J v Victoria (City)*, 2011 BCCA 400.
72. *Safe Streets Act*, SO 1999, c 8.
73. *Safe Streets Act*, SBC 2004, c 75, online: BC Laws <www.bclaws.ca/civix/document/id/complete/statreg/04075_01>.
74. *R v W*, 2016 ONCJ 96.

about himself and his situation.[75] Nonetheless, his *option* to maintain privacy with respect to private matters including his homeless status would have been wiped out by the public nature of the court proceeding. In other cases, individuals have been charged under Ontario's *Safe Streets Act* for soliciting an individual waiting at a bus stop[76] or offering to clean car windows for passing motorists.[77] Although the disclosures in most of these records are limited to the names of the individuals involved and the activities they are charged with undertaking (which by extension label the individuals as street-involved), one of the records goes into much greater detail, revealing highly personal information about the social history and mental health of the individual charged with the offence. In these cases, there is a direct link between marginalized status (homelessness, for example) and the appearance before the courts.

The relationship between vulnerability and involvement is even more direct in the case of human rights tribunals, where it is precisely an experience of alleged discrimination on the basis of protected grounds that brings the individual to the tribunal. Some other tribunals and boards, including the Veterans Appeal Review Board, routinely remove identifying information on the grounds that it is "personal information not relevant to the decision".[78] Likewise, the Social Benefits Tribunal of Ontario holds hearings in private because of the sensitive personal

75. "Ontario Judge Drops $65,000 in Fines Against Former Homeless Man" *Toronto Metro* (4 October 2016), online: Metro News <www.metronews.ca/news/toronto/2016/10/04/judge-drops-65k-in-fines-against-former-homeless-man.html>.
76. *R v F*, 2013 ONCJ 718.
77. *R v B* (2005), 248 DLR (4th) 118 (ONSC).
78. Canada, Veterans Review and Appeal Board, "Decisions" (Ottawa: VRAB, 30 March 2016), online: VRAB <www.vrab-tacra.gc.ca/Decisions/Decisions-eng.cfm>.

information involved in the cases.[79] Many individuals involved in immigration and refugee proceedings are there precisely because they are members of equality-seeking groups. The status of sensitive information revealed in these hearings is complex: proceedings before the Refugee Protection Division and the Refugee Appeal Division are private *unless* decisions are before the Federal Court for judicial review, and proceedings before the Immigration Appeal Division and the Immigration Division are public. Human rights tribunals in Canada, however, default to the identification of parties involved in human rights cases. The Human Rights Tribunal of Ontario ("HRTO"), for example, tells potential applicants that "the hearings and decisions of the HRTO are public except in very special circumstances … and the tribunal's decisions, which include the applicants' names and relevant evidence, are made publicly available through legal reporting services".[80] We will return to the HRTO's practices with respect to anonymization in Part III below.

3. Records Reveal Stigmatizing Information

Open records of human rights tribunal proceedings reveal not only the name of the applicant, but also details of the alleged discrimination including the basis for that alleged discrimination (unless the applicant is successful in taking the often-costly step of seeking a publication ban or some other form of confidentiality order). Thus, for example, in the records of these cases we can come to learn that an applicant suffers from depression, is pregnant, lives with a learning disability, identifies as transgender, or is homeless. These details are not *incidentally* revealed as part of the tribunal proceeding – they are *necessarily* revealed since they

79. Social Justice Tribunals Ontario, "Social Benefits Tribunal: Legislation and Regulation" (Ontario: SJTO, 2015), online: SJTO <www.sjto.gov.on.ca/sbt/legislation-and-regulation/>. Similarly, the Child and Family Services Review Board bans publication of evidence and decisions, and allows only anonymized versions of its decisions to be posted on CanLII, and the Landlord Tenant Board retracts the names of tenants from its decisions before allowing them to be posted on CanLII.

80. Human Rights Tribunal of Ontario, "Frequently Asked Questions" (2015) online: SJTO <www.sjto.gov.on.ca/hrto/faqs>.

often constitute the basis of the claim that is substance of the proceeding. Moreover, the personal information that is exposed in these records leaves the individual vulnerable to *further* discrimination. Thus, public access to these records can contribute to a "vicious cycle" of vulnerability.

The concern is not unfounded. One complainant who was found by the BC Human Rights Tribunal ("BCHRT") to have experienced discrimination based on a mental health issue[81] was in front of that same tribunal seven years later, again alleging discrimination based on mental illness.[82] In that second complaint, which the Tribunal determined was justified, it was alleged that the respondents enacted their discrimination on the basis of information gleaned from the *earlier* human rights case – in other words, their knowledge of the mental illness could at least in part be attributed to an earlier, and public, human rights complaint.[83]

Presumptive openness of court and tribunal records constitutes, for litigants, witnesses, and others named in the court process, *forced* disclosure of personal information. Given the option, people make careful and thoughtful decisions about to whom, when, and where to disclose personal information.[84] This may be particularly true for stigmatizing conditions, where the potential consequences of disclosure include discrimination, social isolation, and even physical danger. Many individuals living with a disability, for example, choose *not* to disclose, in large part for fear of discrimination, especially with respect to employment.[85] Individuals in the work force dealing with mental health issues who choose not to disclose cite fear of discrimination as the primary reason.[86] Many living with positive HIV status carefully balance the psychological advantages

81. *G v The Law Society of British Columbia (No. 4)*, (2009) BCHRT 360.
82. *G v Purewal and another*, (2017) BCHRT 19.
83. *Ibid*.
84. Petronio & Altman, *supra* note 6.
85. Lita Jans, Steve Kaye & Erica C Jones, "Getting Hired: Successfully Employed People with Disabilities Offer Advice on Disclosure, Interviewing, and Job Search" (2012) 22:2 Journal of Occupational Rehabilitation 155.
86. Debbie Peterson, Nandika Currey & Sunny Collings, "'You Don't Look Like One of Them': Disclosure of Mental Illness in the Workplace as an Ongoing Dilemma" (2011) 35:2 Psychiatric Rehabilitation Journal 145.

of disclosure against the costs in terms of stigma and social inclusion.[87] While disclosure of transgender identity can have positive impacts on psychological well-being and personal relationships, it also raises the risk of loss of relationships and even physical violence.[88] Notwithstanding the potential destigmatizing effects,[89] disclosure of a marginalized status can harm the individual involved.[90] It has been compellingly argued that we should not force such disclosures,[91] since the practice could contravene constitutional protections,[92] and might even be considered immoral.[93]

Over-representation of marginalized communities in court and tribunal proceedings, often *because* of the impact of marginalization, combined with the potentially stigmatizing information that is revealed about individuals in court records leaves members of these communities disproportionately vulnerable to further discrimination and other harms. The potential for these harms stand to be exacerbated by widespread publicly-accessible online access to court records. We turn now to examine some of the limited instances in which Canadian law has recognized and responded to this "vicious cycle".

---

87. Geneviève Rouleau, José Côté & Chantal Cara, "Disclosure Experience in a Convenience Sample of Quebec-born Women Living with HIV: A Phenomenological Study" (2012) 12:1 BMC Women's Health 37.
88. M Paz Galupo et al, "Disclosure of Transgender Identity and Status in the Context of Friendship" (2014) 8:1 Journal of LGBT Issues in Counseling 25.
89. See *e.g.* Arjan ER Bos et al, "Mental Illness Stigma and Disclosure: Consequences of Coming Out of the Closet" (2009) 30:8 Issues in Mental Health Nursing 509; Grace J Yoo et al, "Destigmatizing Hepatitis B in the Asian American Community: Lessons Learned from the San Francisco Hep B Free Campaign" (2012) 27:1 Journal of Cancer Education 138.
90. Roberts, *supra* note 29.
91. Talia Mae Bettcher, "Evil Deceivers and Make-Believers: On Transphobic Violence and the Politics of Illusion" (2007) 22:3 Hypatia 43.
92. Anne C Hydorin, "Does the Constitutional Right to Privacy Protect Forced Disclosure of Sexual Orientation" (2003) 30:2 Hastings Constitutional Law Quarterly 237.
93. Susan J Becker, "The Immorality of Publicly Outing Private People" (1994) 73:1 Oregon Law Review 159.

III. Recognition of the Privacy/Vulnerability Cycle in Canadian Law

Notwithstanding that in most cases the privacy of those involved with court proceedings is not protected, our purpose in this section is to identify situations where Canadian law has explicitly or implicitly recognized the privacy/vulnerability cycle as a justification for limiting publication related to, or disclosure within court proceedings involving members of marginalized communities. In tandem with situations in which Canadian courts and legislatures have recognized the privacy/vulnerability cycle in the context of disclosure of information to the *public* about court proceedings, are privacy-justified rules that limit *both* what must be produced in litigation and what can be done with it afterward. We begin by briefly discussing publication bans, which limit *public* access to information about court proceedings, and then turn to case-by-case privilege and deemed/implied undertakings, which impose terms relating to disclosure *within* litigation. In both cases, the law recognizes the privacy/vulnerability cycle and expresses concern about the impact of process-imposed vulnerability on the administration of justice. We note the transition in this law from recognition of a *general* privacy/vulnerability cycle to limited recognition of special risks to specific equality-seeking communities: children and sexual assault survivors in particular. After discussing publication bans, case-by-case privilege and deemed undertakings, we explore other legal manifestations of concern for children and sexual assault survivors before turning to consider more sporadic legal acknowledgments of the privacy/vulnerability cycle relating to other equality-seeking groups. Finally, we consider policy development and commentary focused on the privacy/vulnerability cycle in the context of *online* court records, which supports our concern about the potential for *online* records to exacerbate the cycle for equality-seeking communities.

A. Publication Bans and the Privacy/Vulnerability Cycle

The open court principle is highly venerated in Canadian law. It provides that, as a general rule, court processes and court records should be

publicly accessible. Openness is said to build "public confidence in the integrity of the judicial system by allowing members of the public to hold judges to account".[94] The common law principle in favour of openness is also mirrored in provincial, federal and territorial statutes and policies governing court proceedings.[95] Nevertheless, Canadian courts and legislators have recognized that, in certain circumstances, open access can undermine justice or come at too great a cost to other democratic values in a variety of ways. As a result, certain statutes and common law principles provide for courts and certain other decision-making bodies to determine on a case-by-case basis whether there should be an exception to that rule. These case-by-case decisions are to be made with reference to the Supreme Court of Canada's decisions in two seminal cases relating to publication bans, *R v Mentuck*[96] and *Dagenais v Canadian Broadcasting Corp*.[97]

In *Mentuck*, the Supreme Court of Canada held that a publication ban should only be issued where:

> (a) such an order is necessary in order to prevent a serious risk to the proper administration of justice because reasonably alternative measures will not prevent the risk; and
>
> (b) the salutary effects of the publication ban outweigh the deleterious effects on the rights and interests of the parties and the public, including the effects on the right to free expression, the right of the accused to a fair and public trial, and the efficacy of the administration of justice.[98]

In *Dagenais*, the Supreme Court of Canada pointed to a long list of competing considerations of sufficient weight to warrant a publication ban. At least three of these implicitly recognize the way in which a lack

---

94. Bailey & Burkell, *supra* note 2 at 152.
95. See *e.g. Courts of Justice Act*, RSO 1990, c C43, ss 135, 137; Provincial Court of British Columbia, "Access to Court Records" Policy Code ACC-2 (British Columbia: 28 February 2011) online: Provincial Court BC <www.provincialcourt.bc.ca/downloads/public%20and%20media%20access%20policies/ACC-2%20-%20Access%20to%20Court%20Records.pdf>
96. 2001 SCC 76 [*Mentuck*].
97. [1994] 3 SCR 835 [*Dagenais*].
98. *Mentuck*, *supra* note 96 at para 32.

of privacy can exacerbate inequality and vulnerability, namely: protecting vulnerable witnesses (*e.g.* children, sexual assault complainants); reducing the stigma of conviction for young offenders, thereby increasing the possibility of rehabilitation; and encouraging reporting of sexual offences by reducing the fear of notoriety of becoming a complainant.[99]

The issues of protecting children and targets of sexual violence came together in *AB v Bragg*.[100] The Supreme Court of Canada held that a teen girl who sought a publication ban on the content of a Facebook page in which she was subjected to "sexualized cyberbullying", should be allowed to proceed using a pseudonym on a preliminary application for disclosure.[101] Relying on the decisions in *Dagenais* and *Mentuck*, and noting research showing that "allowing the names of child victims and other identifying information to appear in the media can exacerbate trauma, complicate recovery, discourage future disclosures, and inhibit cooperation with authorities",[102] as well as the lasting harms of the publicity of sexualized online attacks, Abella J, writing for the Court, concluded:

> If we value the right of children to protect themselves from bullying, cyber or otherwise, if common sense and the evidence persuade us that young victims of sexualized bullying are particularly vulnerable to the harms of revictimization upon publication, and if we accept that the right to protection will disappear for most children without the further protection of anonymity, we are compellingly drawn in this case to allowing A.B.'s anonymous legal pursuit of the identity of her cyberbully.[103]

Here the Court explicitly recognized the "vicious cycle" of a lack of privacy and the "*inherent* vulnerability of children".[104] In addition, Abella J noted that "[i]n the context of sexual assault, this Court has already recognized that protecting a victim's privacy encourages reporting".[105] In this way, the cycle of gender inequality and lack of privacy in court proceedings

99. *Dagenais*, *supra* note 97 at paras 883-84.
100. 2012 SCC 46 [*Bragg*].
101. *Ibid* at paras 22, 26.
102. *Ibid* at para 26.
103. *Ibid* at para 27.
104. *Ibid* at para 17 [emphasis in original].
105. *Ibid* at para 25.

is evident, although the Court did not explicitly discuss the plaintiff's situation in these terms. The plaintiff had already suffered a sexualized online attack (which included someone impersonating her and posting a photo of her), a kind of attack disproportionately suffered by women and girls, who are also more likely to be shamed in relation to exhibitions of their sexuality.[106] A refusal to grant AB a degree of privacy in relation to her legal proceeding would have re-subjected her to further gendered scrutiny and attack – a classic illustration of the "vicious cycle" between the vulnerability of marginalized populations and a lack of privacy in court proceedings. Although AB was ultimately able to proceed under a pseudonym, her right to do so came at the cost of appeals all the way to the Supreme Court of Canada – a price most people, particularly those from many marginalized communities, are unlikely to be able to pay.

B. Case-by-case Privilege and Deemed/Implied Undertakings

In contrast with publication bans, which focus solely on public access to information about court proceedings, case-by-case privilege and deemed/implied undertakings impose limits relating to procedures internal to litigation. In both cases the focus is on balancing privacy with other kinds of public interests. In some cases, Canadian courts explicitly or implicitly connect privacy with vulnerability, and the risk that exposing litigants to too much vulnerability will jeopardize their right and ability to seek legal remedies. Thus, despite the truth-finding goal of litigation and the idea that disclosure of all relevant information best serves that goal, parties need not produce *all* relevant documents within litigation. As the British Columbia Court of Appeal, per Southin JA, noted in *Interclaim Holdings Limited v Down*:

> Suffice it to say that, in my opinion, … the notion that everybody is entitled to have access to everything filed in civil proceedings … in contradistinction to having the right to be present at every proceeding in which a final judgment is sought should be canvassed again. A legal system which has no decent respect

106. Jane Bailey, "'Sexualized Online Bullying' Through an Equality Lens: Missed Opportunity in *AB v. Bragg*?" (2014) 59:3 McGill Law Journal 709.

> for the privacy of litigants is as tyrannical as a legal system in which rights are determined behind closed doors.[107]

Documents subject to privilege represent an important exception to the general disclosure rule.[108] While the traditional categories of privilege protect the solicitor-client relationship (solicitor-client privilege) and the process of litigation (litigation privilege), in *Slavutych v Baker et al*, the Supreme Court of Canada confirmed that those categories are not closed[109] and adopted a four-part test for determining on a case-by-case basis whether materials claimed to be confidential should be exempt from disclosure. This privilege applies to communications that: (i) originate in confidence; (ii) where confidence is essential to the relationship in which the communication arose; (iii) that relationship is one that should be "sedulously fostered; and (iv) the interests served by protecting against disclosure outweigh the interest in getting at the truth to correctly resolve the litigation.[110]

In applying this four-part test in the context of a civil sexual assault case in *M(A) v Ryan*, where the defendant sought production of records from the plaintiff's psychiatrist, the Supreme Court of Canada found that if psychiatrist-patient confidence was broken, it could jeopardize a patient's willingness to seek treatment.[111] Justice McLachlin (as she was then) writing for the majority, noted that such an outcome was to be avoided, especially in the context of survivors of "sexual abuse [who] often suffer trauma, which, left untreated, may mar their entire lives".[112] In reaching this conclusion, the Court relied on constitutional protections for privacy *and* equality, noting:

> A rule of privilege which fails to protect confidential doctor/patient communications in the context of an action arising out of sexual assault perpetuates the disadvantage felt by victims of sexual assault, often women. The

---

107. 2003 BCCA 266 at 32.
108. Although the existence of relevant documents over which privilege is claimed must be disclosed. See *e.g. Ontario Rules of Civil Procedure*, RRO 1990, Reg 194, s 30.02(1) [*Ontario Rules of Civil Procedure*].
109. *Slavutych v Baker et al*, [1976] 1 SCR 254.
110. *M(A) v Ryan*, [1997] 1 SCR 157 at para 20 [*M(A)*], referring to *Slavutych.*
111. *Ibid* at paras 25-26.
112. *Ibid* at para 27.

> intimate nature of sexual assault heightens the privacy concerns of the victim and may increase, if automatic disclosure is the rule, the difficulty of obtaining redress for the wrong. The victim of a sexual assault is thus placed in a disadvantaged position as compared with the victim of a different wrong. The result may be that the victim of sexual assault does not obtain the equal benefit of the law to which s. 15 of the *Charter* entitles her. She is doubly victimized, initially by the sexual assault and later by the price she must pay to claim redress.[113]

McLachlin J also rejected the argument that a plaintiff forfeits the right to privacy by commencing litigation, finding:

> I accept that a litigant must accept such intrusions upon her privacy as are necessary to enable the judge or jury to get to the truth and render a just verdict. But I do not accept that by claiming such damages as the law allows, a litigant grants her opponent a licence to delve into private aspects of her life which need not be probed for the proper disposition of the litigation.[114]

This reasoning subsequently carried over into analysis of the privacy rights of sexual assault complainants in the context of the deemed undertaking.

The deemed and implied undertaking rules[115] generally prohibit disclosure of "pre-trial documentary and oral discovery for purposes other than the litigation in which it was obtained".[116] Although these rules do not place similar restrictions on documentary and oral discovery that make their way into the public record during trials or motions, they nevertheless reflect recognition of the privacy/vulnerability cycle and its potential impact on the administration of justice. In *Juman v Doucette*, the Supreme Court of Canada, per Binnie J, pointed to privacy protection as one of two related rationales for these undertakings:

> The public interest in getting at the truth in a civil action outweighs the examinee's privacy interest, but the latter is nevertheless entitled to a measure of protection. The answers and documents are compelled by statute solely for the purpose of the civil action and the law thus requires that the invasion of privacy should generally be limited to the level of

113. *Ibid* at para 30.

114. *Ibid* at para 38.

115. The implied undertaking exists as a product of common law, while deemed undertakings are typically reflected in provincial Rules of Civil Procedure. See *e.g. Ontario Rules of Civil Procedure*, *supra* note 108, s 30.1.

116. *Juman v Doucette*, 2008 SCC 8 at 21.

> disclosure necessary to satisfy that purpose and that purpose alone. ... There is a second rationale supporting the existence of an implied undertaking. A litigant who has some assurance that the documents and answers will not be used for a purpose collateral or ulterior to the proceedings in which they are demanded will be encouraged to provide a more complete and candid discovery.[117]

That the imposition of such limits can be of particular importance in the context of civil and criminal proceedings relating to sexual assault was recognized at first instance in *SC v NS* where the defendant in a criminal sexual assault trial used documents produced by the complainant in a civil sexual assault proceeding in order to impeach her during her testimony at the criminal trial.[118] The Court's finding that the deemed undertaking prevented the defendant from using the documents in another proceeding without first seeking leave of the court was overturned on appeal. However, the observations of Matheson J with respect to privacy remain apt. Justice Matheson rejected the defendant's argument that the plaintiff had given up her right to privacy by initiating the civil action, reasoning:

> If that choice defeated all privacy interests, the deemed undertaking would not exist. Instead, the court and the *Rules of Civil Procedure* have acknowledged that plaintiffs remain entitled to some measure of protection of their privacy and are entitled to limitations on the use of their discovery evidence outside the proceedings for which the discovery was compelled.[119]

Finding that "[t]he primary concern underlying the undertaking is the protection of privacy – discovery is an invasion of the right of an individual to keep one's evidence and documents to oneself",[120] Matheson J went on to note the privacy/vulnerability cycle recognized in *Criminal Code*[121] restrictions on use of complainant's medical or counselling records in a sexual assault trial. In particular, she noted that parliamentary adoption of those restrictions and a detailed process for determining whether such records could be used:

---

117. *Ibid* at paras 25-26.
118. 2017 ONSC 353; overturned 2017 ONSC 556 [*SC*].
119. *Ibid* at para 80.
120. *Ibid* at para 39.
121. RSC 1995, c C-46 [*Criminal Code*].

> Parliament has recognized that the compelled production of personal information may deter complainants of sexual offences from reporting the events to police and from seeking the necessary treatment, counselling or advice; that production may breach a person's right to privacy and equality; and that the production to the accused of such information may be necessary in order for an accused to make full answer and defence.[122]

We turn now to discuss specific exceptions to openness in relation to children and sexual assault complainants found elsewhere in Canadian law in order to highlight the role that recognition of the privacy/vulnerability cycle plays in relation to each, paying particular attention to explanations for exceptions that connect privacy, vulnerability and membership in equality-seeking communities.

C. Children and the Privacy/Vulnerability Cycle

The connection between the privacy/vulnerability cycle and marginalization is most consistently demonstrated in Canadian law with respect to the protection of children in court proceedings. Here we provide examples from two areas: child welfare and family law proceedings, and the *Youth Criminal Justice Act* ("*YCJA*").[123]

1. Child Welfare and Family Law Proceedings

In addition to the examples discussed in part A above, Canadian courts also connect privacy with the vulnerability of children in the context of provincial child welfare legislation[124] and in family law proceedings.[125] Although child welfare legislation can incorporate both provisions that initially presume in favour of openness *and* those that initially presume against openness, here we focus on the former. In *Chatham-Kent Children's Services v AH*, the Ontario Superior Court of Justice allowed a media request to vary an order excluding the public from a hearing by allowing access to a redacted copy of the transcript of an *in camera* hearing in

122. *SC*, *supra* note 118 at para 95.
123. SC 2002, c 1 [*YCJA*].
124. See *e.g. Child and Family Services Act*, RSO 1990, c C11, s 45(8); *Child and Family Services Act*, SS 1989-90, c C-7.2, s 26 [*CFSA*].
125. See *e.g. Provincial Court Act*, RSBC 1996, c 379, s 3(6) [*Provincial Court Act*].

a child protection proceeding involving the disappearance of several children who had been apprehended from the jurisdiction.[126] Although citing *Bragg*, and other criminal and family law cases, Templeton J noted that the case before him was not a criminal, civil matter or family law matter, but a child protection proceeding. He concluded that restrictions on public access to the transcript were necessary because:

> in certain circumstances, the protection of a vulnerable child and that child's privacy may well go beyond merely the name of the child in protection proceedings. Children who are the subject of an application by the state for intervention are also allegedly vulnerable in their environment at home, at school and/or in their neighbourhood. They are subject to the conduct and attitudes of the adults who interact with them. Disclosure to others of the intimacy of their lives is beyond their control. Without the ability or opportunity for critical thought, they are swept into a process of the balancing of rights of others and in that process, it can be difficult to hear their voice. ... In other words, the child's world and privacy are inextricably linked to an investigation of the parent's.[127]

As a result, Templeton J concluded that in child protection matters, "the need to shield a vulnerable child rests not only on the child's chronological age but also and perhaps more significantly, the factual circumstances in which the child lives or has been placed".[128]

In contrast, while citing similar authorities to those relied upon in *AH*, the Saskatchewan Court of Queen's Bench, per Rothery J, concluded in the context of child protection proceedings in *R(MN) v Saskatchewan (Minister of Social Services)* that the CBC could publish the name of a parent accused of harming her children, provided that they gave advanced notice of the broadcast to the Department of Social Services in the area where her children resided.[129] Rothery J found that although section 26(2) of the *Child and Family Services Act*[130] permitted publication bans where publication would not be in the best interests of a child involved in the hearing or would likely identify a child, "[t]he court is not permitted to weigh the effect of the publication on the parents of the child. Thus,

126. 2014 ONSC 1697 [*AH*].
127. *Ibid* at paras 42-43.
128. *Ibid* at para 44.
129. (1999), 179 Sask R 238, (QB) at para 28 [*R(MN)*].
130. *CFSA*, *supra* note 124.

unless the publication of the parent's name affects the child, there is no justification for the limitation of the freedom of expression".[131]

Meanwhile, in British Columbia, rules of court impose stringent restrictions on public access to court records relating to child welfare proceedings, family law cases and separation agreements,[132] and various statutes restrict publication of information in family and children's matters that would likely disclose the identity of a child or party.[133] As a result, although BC offers the most extensive online access to court records in Canada through Court Services Online ("CSO"),[134] public access is available only in relation to civil and criminal cases (with certain exceptions discussed further below), and *not* in relation to family law cases.

2. Youth Criminal Justice Act

The *YCJA* came into effect in 2003, replacing the *Young Offenders Act*, which had been in place since 1984.[135] The *YCJA* creates a specialized framework for dealing with children under the age of 12 and young people between the ages of 12 and 18 who are involved in criminal offences.[136] It recognizes society's responsibility to "address the developmental challenges and the needs of young persons and to guide them into adulthood", as well as the "special guarantees" of children's and young people's rights and freedoms, and the goal of "effective rehabilitation and reintegration" of

131. *R(MN)*, *supra* note 129 at para 26.
132. British Columbia, "Court Record Access Policy" (Vancouver: Supreme Court of British Columbia, 2011) at 21, online: <www.courts.gov.bc.ca/supreme_court/announcements/BCSC%20Court%20Record%20Access%20Policy%20-%20February%2014%202011.pdf>.
133. See *e.g. Provincial Court Act*, *supra* note 125, s 3(6).
134. British Columbia, "Welcome to Court Services Online" Court Services Online, Version 3.0.0.04, online: Courts of British Columbia <https://justice.gov.bc.ca/cso/index.do>.
135. Canada, Department of Justice, "Canadian Youth Justice Legislation: A Chronology" (Ottawa: Department of Justice, 2015), online: DOJ <www.justice.gc.ca/eng/cj-jp/yj-jj/tools-outils/sheets-feuillets/yjc-jaac.html>.
136. *YCJA*, *supra* note 123, s 2(1).

young people into society after involvement in criminal proceedings.[137]

Restrictions relating to publication, records and information about young people are imposed in Part 6 of the *YCJA* as one means of addressing these objectives. For example, section 110(1) prohibits (subject to specific exceptions) publication of the name of any young person dealt with under the *YCJA*, or any other information about them that would identify them, while later sections in Part 6 impose limitations on creation, access to, and destruction of records related to *YCJA* investigations and proceedings involving young people.[138] Generally, breach of the publication ban is a criminal offence.[139] According to the Department of Justice:

> The rationale for protecting the privacy of young persons through publication bans is in recognition of their immaturity and the need to protect them from the harmful effects of publication so that their chances of rehabilitation are maximized.[140]

The cycle connecting privacy, vulnerability and youth is explored in some detail in a number of Canadian cases and has been reiterated frequently in parliamentary debate.[141]

In *FN (Re)* the Supreme Court of Canada found that section 110(1) protected already vulnerable youth made more vulnerable by publication, while at the same time achieving broader societal goals. Writing for the Court, Binnie J, noted:

> Stigmatization or premature "labeling" of a young offender still in his or her formative years is well understood as a problem in the juvenile justice system. A young person once stigmatized as a lawbreaker may, unless given help and redirection, render the stigma a self-fulfilling prophecy. In the long run, society

137. *Ibid*, preamble.
138. *Ibid*, ss 110-29.
139. *Ibid*, s 110.
140. Canada, Department of Justice, "Publication Bans" (Ottawa: Department of Justice, 2015), online: DOJ <www.justice.gc.ca/eng/cj-jp/yj-jj/tools-outils/sheets-feuillets/publi-publi.html>.
141. See *e.g. House of Commons Debates*, 37th Parl, 1st Sess, Vol 137, No 067 (29 May 2001) at 4343 (Odina Desrochers); *House of Commons Debates*, 37th Parl, 1st Sess, Vol 137, No 036 (26 March 2001) at 2217 (Reg Alcock); *House of Commons Debates*, 37th Parl, 1st Sess, Vol 137, No 036 (26 March 2001) at 2217 (Ken Epp).

> is best protected by preventing recurrence. Lamer CJ, in Dagenais … pointed out in another context that non-publication is designed to "maximize the chances of rehabilitation for "young offenders"".[142]

Abella J, writing for the majority in *R v DB* the Supreme Court of Canada, cited social science research and international instruments recognizing the negative impact of media on young people, in support of the conclusion that the *YCJA* restrictions on publication afforded necessary protection to youth because of the "greater psychological and social stress" they would be vulnerable to upon publication.[143] The majority cited expert testimony before the Standing Committee on Justice that indicated that "you'd be hardpressed to find a single professional who has worked in this area who would be in favour of the publication of names", and appellate authority from Quebec and Ontario emphasizing the "damage" that "stigmatizing and labelling" a young person could do to their self-image and self-worth.[144] In light of this, the majority, per Abella J, found that lifting a ban on publication should be seen as an element of sentencing that "renders the sentence more severe".[145] However, the majority also tied the right to privacy protection to a presumed "diminished moral culpability" of young persons, noting that children's "lack of experience with the world warrants leniency and optimism for the future", and concluding that "offenders who act out of immaturity, impulsiveness, or other illconsidered motivation are not to be dealt with as if they were proceeding with the same degree of insight into their wrongdoing as more mature, reflective, or considered individuals".[146] Obviously, this particular aspect of the explanation of the privacy/vulnerability cycle cannot and should not be extended to adults from other equality-seeking groups.

Relying in part on *DB*, the Ontario Court of Justice, per Cohen J,

---

142. 2000 SCC 35 at para 14.
143. 2008 SCC 25 at para 87 [*DB*].
144. *Ibid* at paras 84-85.
145. *Ibid* at para 87.
146. *Ibid* at para 62-63, quoting, respectively, Allan Manson, *The Law of Sentencing* (Toronto: Irwin Law, 2001) at 103-04 and Gilles Renaud, *Speaking to Sentence: A Practical Guide* (Toronto: Carswell, 2004) at 10.

in *Toronto Star Newspaper Ltd v Ontario* pointed to the *YCJA* restrictions on publication as one indication that the proper administration of justice requires consideration of young people's privacy rights.[147] Cohen J denied a media request for access to victim impact statements and pre-sentence reports in three cases involving young offenders convicted of serious crimes. She found that the *YCJA* publication restrictions were connected to the presumed diminished moral culpability of young people, but were also rooted in protecting their "dignity, personal integrity and autonomy" as required by the *Convention on the Rights of the Child* and the *Canadian Charter of Rights and Freedoms*.[148] The reasoning in *Toronto Star*, which the Supreme Court of Canada cited with approval in *Bragg*,[149] has also been relied upon by other Ontario courts as a touchstone for protecting young people when determining whether court-connected materials relating to them ought to be disclosed.[150]

D. Sexual Assault Complainants and the Privacy/Vulnerability Cycle

A number of *Criminal Code* provisions that connect the privacy/vulnerability cycle with inequality relate to sexual assault complainants. Here we focus on two such provisions: prohibition of the publication of identifying information about sexual assault complainants and restrictions on the use of complainants' past sexual history at trial.

1. Prohibitions on Publication of Identifying Information

The *Criminal Code* includes numerous provisions that initially presume in favour of openness, but grant judges discretion to impose restrictions relating to hearings and publication of identifying information. For

147. 2012 ONCJ 27 at paras 33-48 [*Toronto Star*].
148. *Ibid* at paras 43-47. See: *Convention on the Rights of the Child*, 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990); *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.
149. *Bragg*, *supra* note 100 at para 18.
150. See *e.g. R v Beckford and Stone*, 2012 ONSC 7365; *Chief of Police v Mignardi*, 2016 ONSC 5500.

example, under section 486.31 a judge *may*, on application by the prosecutor or a witness, order non-disclosure of a witness' identity.[151] Under section 486.4 a judge *may* order non-disclosure of information that could identify a witness or victim in the context of proceedings involving sexual offences.[152] However, under section 486.4(2), a judge *must* order non-disclosure of identifying information relating to a witness under 18 or a victim in proceedings involving sexual offences if the witness, victim or prosecutor applies for such an order.[153] In considering the constitutionality of this provision in *Canadian Newspapers Co v Canada (Attorney General)*,[154] the Supreme Court of Canada connected the cycle of privacy and vulnerability to the broader societal objective of encouraging reporting of widely under-reported sexual offences. Lamer J (as he then was), writing for the Court, noted:

> In the present case, the impugned provision purports to foster complaints by victims of sexual assault by protecting them from the trauma of wide-spread publication resulting in embarrassment and humiliation. Encouraging victims to come forward and complain facilitates the prosecution and conviction of those guilty of sexual offences. Ultimately, the overall objective of the publication ban ... is to favour the suppression of crime and to improve the administration of justice.[155]

In this way, the Court recognized the connection between privacy and vulnerability, finding that it weighed in favour of imposing limitations on publication. However, it tied the concern about protecting against vulnerability to goals relating to the administration of justice, rather than to protecting the privacy rights of an equality-seeking group *per se*. This, combined with the fact that the *Criminal Code* provision permits the decision about publication to be taken out of a sexually assaulted woman's hands by allowing the prosecutor to make the application, raises questions about how effectively it addresses the privacy/vulnerability cycle for women, who are disproportionately likely to be victims of sexual

151. *Criminal Code*, *supra* note 121, s 486.31.
152. *Ibid*, s 486.4.
153. *Ibid*, s 486.4(2).
154. [1988] 2 SCR 122.
155. *Ibid* at para 15.

violence.[156]

2. Restrictions on the Use of Complainants' Past Sexual History

The *Criminal Code* also addresses the privacy rights of sexual assault complainants by imposing limits on use of the complainant's past sexual history. Section 276 of the *Criminal Code*, requires an accused who seeks to bring forward the past sexual history of a complainant in a sexual assault case to first bring a motion for leave to do so.[157] In deciding whether to allow such evidence, the court must consider, among other things, "the need to remove from the fact-finding process any discriminatory belief or bias" and "the potential prejudice to the complainant's personal dignity and right of privacy".[158] Publication, broadcast or transmission of information relating to the application is prohibited unless the evidence is determined admissible or the judge orders the determination and reasons to be published.[159] While it is at best unclear whether this provision is actually applied in a way that positively affects equality,[160] the reasoning underlying the provision *does* connect privacy, vulnerability and equality.

In *R v Mills*[161] the Court, referring to its reasons in *M(A)* (discussed above in Part III.B)., upheld the constitutionality of *Criminal Code* amendments that protected against what Justice L'Heureux-Dubé had previously referred to as "extensive and unwarranted inquiries into the past histories and *private lives* of complainants of sexual assault", a practice she said "indulges the discriminatory suspicion that women

156. For further discussion, see Jane Doe, "What's in a Name? Who Benefits from the Publication Ban in Sexual Assault Trials?" in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009) 265.

157. *Criminal Code*, *supra* note 121, s 276.

158. *Ibid*, s 276(3)(d), (f).

159. *Ibid*, s 276.3.

160. For further discussion see Lise Gotell, "When Privacy is not enough: Sexual Assault Complainants, Sexual History Evidence and the Disclosure of Personal Records" (2006) 43:3 Alberta Law Review 743.

161. [1999] 3 SCR 668 [*Mills*].

and children's reports of sexual victimization are uniquely likely to be fabricated".[162] Noting privacy's "underlying values of dignity, integrity and autonomy",[163] McLachlin and Iacobucci JJ, writing for the majority in *Mills*, went on to connect the privacy/vulnerability cycle to equality in the context of compelled disclosure in court proceedings:

> When the boundary between privacy and full answer and defence is not properly delineated, the equality of individuals whose lives are heavily documented is also affected, as these individuals have more records that will be subject to wrongful scrutiny. Karen Busby cautions that the use of records to challenge credibility at large will subject those whose lives already have been subject to extensive documentation to extraordinarily invasive review. This would include women whose lives have been documented under conditions of multiple inequalities and institutionalization such as Aboriginal women, women with disabilities, or women who have been imprisoned or involved with child welfare agencies.[164]

E. Other Equality-Seeking Groups and the Privacy/Vulnerability Cycle

Although Canadian law involving young persons and sexual assault complainants more consistently (but certainly not *always*) acknowledges the privacy/vulnerability cycle and its connection to equality, there is at least a limited recognition of the cycle in relation to certain other equality-seeking groups. This pattern is repeated in the human rights tribunal cases to which we now turn.

As discussed in Part II.B.2. above, certain court and tribunal rules and procedures also recognize and attempt to mitigate the "vicious cycle" of privacy loss and vulnerability, although the rationale for defaulting in favour of access in some cases where clearly vulnerable community members are involved and not in others involving equally vulnerable participants remains unclear. Nonetheless, here we explore HRTO practices that suggest privacy/vulnerability rationales for limiting access

---

162. *R v O'Connor*, [1995] 4 SCR 411 at paras 122-23 [emphasis added].
163. *Mills*, *supra* note 161 at paras 80-81 [emphasis omitted].
164. *Ibid* at para 92, citing Karen Busby, "Discriminatory Uses of Personal Records in Sexual Violence Cases" (1997) 9:1 Canadian Journal of Women and the Law 148 at 161-62.

to records and/or proceedings.

As noted above, human rights proceedings, based as they are on claims related to social locations that render individuals and groups vulnerable to discrimination, would seem to provide classic examples of situations in which the privacy/vulnerability cycle is likely be at play. Many human rights tribunals in Canada are authorized to preclude public access to hearings and to limit access to their case files on a case-by-case basis.[165] Hearings before the HRTO, for example, "are open to the public" unless the Tribunal orders otherwise,[166] and all written decisions are publicly available.[167] The HRTO *may* order protection of the "confidentiality of personal or sensitive information where it considers it appropriate to do so", but unless otherwise ordered, in its decisions it *must* use initials to identify children under 18 and the representative of children under 18 in the proceeding.[168] HRTO's practice direction states anonymization of decisions will *only* happen in two circumstances: to protect children's identity or in "exceptional circumstances".[169] As such, we again see a prioritization of children's privacy.

MacDonnell's analysis of HRTO decisions relating to requests for confidentiality suggest that success in such cases is more likely for

---

165. See *e.g.* Alberta Human Rights Commission, *Procedural Manual for Tribunal Hearings*, at 10-11, online: ABHRC <https://www.albertahumanrights.ab.ca/Documents/Procedural_Manual_September_2015.pdf>; British Columbia Human Rights Tribunal, *Rules of Practice and Procedure*, Rule 5, online: BCHRT <www.bchrt.bc.ca/shareddocs/rules/RulesOfPracticeAndProcedure.pdf >.
166. Human Rights Tribunal of Ontario, *Rules of Procedure*, Rule 3.10, online: <www.sjto.gov.on.ca/documents/hrto/Practice%20Directions/HRTO%20Rules%20of%20Procedure.html#3>.
167. *Ibid*, Rule 3.12.
168. *Ibid*, Rule 3.11, 3.11.1. The HRTO *may* also use initials for other parties if it is necessary to protect a child's identity, at Rule 3.11.1.
169. Human Rights Tribunal of Ontario, *Practice Direction on Anonymization of HRTO Decisions*, online: SJTO <www.sjto.gov.on.ca/documents/hrto/Practice%20Directions/Anonymization %20of%20HRTO%20Decisions.html>.

minors, applicants claiming sexual harassment,[170] and where a ban has issued in a related criminal case. Anonymization has also been ordered in a handful of cases where the sexual orientation or gender identity of the applicant was in issue.[171] In contrast, confidentiality requests in cases involving claims related to race, ethnic origin, creed, place of origin or ethnic origin, or which raised the issue of reprisal were unsuccessful, while requests in cases involving disability produced mixed results.[172] In a case decided after MacDonnell's analysis, a request on the basis of being a recipient of social assistance was rejected.[173]

The HRTO imposes a high standard for obtaining confidentiality with respect to disability, notwithstanding social science evidence documenting the continuing stigma attached to mental illness and the negative employment, insurance, parenting and other life repercussions that can result from disclosure of mental illness.[174] For example, in *K v Northern Initiative for Social Action*, the HRTO concluded that "[a] general claim that there is still stigma associated with mental illness is insufficient" to justify anonymization.[175] In light of this approach, it seems logical to suggest that those who prefer not to have their disabilities publicly disclosed in HRTO decisions will be deterred from seeking relief,[176] just as the Supreme Court of Canada in *Bragg* found child victims of "online sexualized cyberbullying" were likely to be deterred from seeking a legal remedy in the absence of some form of

---

170. MacDonnell, *supra* note 2. However, anonymization in sexual harassment cases is not automatic: *B v H*, 2012 HRTO 212.
171. MacDonnell, *ibid* at 115-8.
172. *Ibid* at 118-9.
173. *C v Ontario (Community and Social Services)*, 2016 HRTO 691. This decision seems particularly paradoxical in light of the fact that the Social Benefits Tribunal of Ontario (and indeed all other Social Justice Tribunals in Ontario other than the HRTO) anonymize their decisions in some way: MacDonnell, *supra* note 2 at 136.
174. MacDonnell, *ibid* at 122-123.
175. 2014 HRTO 136 at para 9. See also *F v Toronto Transit Commission*, 2017 HRTO 514 at paras 27-28; *K v Toronto Police Service*, 2012 HRTO 1374 at para 20.
176. MacDonnell, *supra* note 2 at 125.

confidentiality.[177] Deterring claims by those who prefer not to disclose their disabilities arguably undermines their right to equal benefit and protection of the law in the same way that disclosure of the identities of sexual assault complainants without their consent triggers their equality rights, as found by the Supreme Court of Canada in *Mills*.[178]

Notwithstanding concerns around HRTO practice in relation to disability and certain other grounds of discrimination, in situations where the HRTO *does* decide to order anonymization of its decisions, its reasons sometimes acknowledge the privacy/vulnerability cycle. In *GG v 1489024 Ontario Ltd*, for example, the HRTO ordered anonymization in a case involving allegations of sexual harassment.[179] Although Adjudicator Whist noted that the mere fact that "issues of a personal or sensitive nature" would not be enough to justify anonymization, he concluded that the case fell "within one of the exceptional situations" where anonymization was appropriate, citing a "risk of disclosure of highly sensitive information" in a case where the applicant had "already been subject to a sexual assault arising out of the facts that form the basis" for her complaint.[180]

F. The Privacy/Vulnerability Cycle and Online Court Records: Commentary and Policy

Policymakers have also articulated concerns about the privacy/vulnerability cycle in considering the implications of online accessibility of court records. In British Columbia, for example, the Provincial Court issued a direction to prevent remote online access to non-conviction information,

177. *Bragg*, *supra* note 100.
178. *Criminal Code*, *supra* note 121, ss 486.31, 486.4, 486.4(2).
179. 2012 HRTO 824.
180. *Ibid* at para 9.

stays of proceedings and peace bonds after specific periods of time.[181] The direction specifically refers to submissions filed as part of a public consultation on the issue that illustrate the privacy/vulnerability cycle and unjust stigma arising from the use of non-conviction information to judge individuals' suitability for jobs and rental accommodation.[182] Justice Bielby of the Alberta Court of Queen's Bench expressed similar concerns about allowing "ready public access to the names of unconvicted accused" in *Krushell*, noting that:

> [s]tatutorily prescribed punishments for the convicted would pale in many cases in comparison to the de facto punishment created by posting [such] information… for the benefit of the gossip and the busybody.[183]

In light of these concerns, the Court rejected an access to information request for disclosure of daily court dockets by an applicant who proposed to post them on the internet. Additionally, courts in BC and Alberta have chosen not to post certain kinds of decisions on their websites, such as those relating to family law, child protection and divorce,[184] and, as noted above, family court records are not publicly accessible on BC's CSO.

The Office of the Privacy Commissioner of Canada ("OPC") has also issued access guidelines for federal tribunals governed by the *Privacy Act*[185] with respect to addressing the privacy/vulnerability cycle aggravated by

---

181. Memorandum from the Provincial Court of British Columbia (March 2016) Policy regarding criminal court record information available through Court Services Online, at 7, online: Provincial Court BC <www.provincialcourt.bc.ca/downloads/NewsReleases/Provincial%20Court%20Post-Consultation%20Memorandum%20-%20CSO%20Criminal%20Information.pdf>. Non-conviction information has to be removed within 30 days of the entry of the acquittal, withdrawal or dismissal. Information on stays of proceedings has to be rendered inaccessible 1 year after entry of the stay. Information relating to peace bonds has to be rendered inaccessible once the bond has expired.
182. *Ibid* at 3-4.
183. *Alberta (Attorney General of) v Krushell*, 2003 ABQB 252 at para 49 [emphasis omitted].
184. Gary Dickson QC, "Administrative Tribunals, Privacy and the Net" (2009) 6:12 Canadian Privacy L Rev 65 at 73, online: Perma <https://perma.cc/A9L9-59C7>.
185. RSC 1985, c P-21.

online access to court records noting:

> When personal information is made available on the internet, individuals are at greater risk of identity theft, stalkers, data profilers, data miners and *discriminatory practices*; personal information can be taken out of context and used in illegitimate ways; and individuals lose control over personal information they may well have legitimately expected would be used for only limited purposes.[186]

Additionally, the OPC has questioned whether "the broad public needs to know the names of individuals involved or requires access to intimate personal details through decisions posted widely on the internet",[187] expressing the view that "the right to open courts does not outweigh the right to privacy" so that both should exist in equilibrium.[188] In line with these concerns, in 2008, the OPC recommended that Service Canada should either depersonalize or post only summaries of the Office of the Umpire decisions on the internet, noting that these appeals related to personal information about employment insurance.[189]

Similarly, the Saskatchewan Information Privacy Commissioner ("IPC") recommended that the Automobile Injury Appeal Commission mask the identity of applicants before posting their decisions online.[190] Subsequently, the IPC's 2004-5 annual report highlighted the connection between online disclosure of personal and health information and "such

---

186. Office of the Privacy Commissioner of Canada, "Guidance Document: Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals" (February 2010) at 2, online: OPC <publications.gc.ca/collections/collection_2013/priv/IP54-48-2010-eng.pdf> [emphasis added].
187. Jennifer Stoddart, "Setting the 'Bar' on Privacy Protection" (speech delivered at the Canadian Bar Association Legal Conference and Expo, Quebec City, 17 August 2008), online: OPC <https://www.priv.gc.ca/en/opc-news/speeches/2008/sp-d_080817/>.
188. Canadian Judicial Council, "Synthesis on the Comments on the JTAC's Discussion Paper on Open Courts Electronic Access to Court Records and Privacy", by Lisa Austin & Frederic Pelletier (Ottawa: January 2005) at 10, online: CJC <https://www.cjc-ccm.gc.ca/cmslib/ general/news_pub_techissues_Synthesis_2005_en.pdf>.
189. Dickson, *supra* note 184 at 66.
190. *Ibid* at 78.

problems as identity theft, marketing opportunities, commercial data bases, personal safety of victims of domestic violence and stalking".[191] Ultimately, the Commission adopted a policy of using initials in its decisions.[192]

In 2005 the Canadian Judicial Council's Judges Technology Advisory Committee issued its *Model Policy for Access to Court Records in Canada*.[193] That policy stated that it did not endorse making all court records accessible online, and specifically adverted to the privacy/vulnerability cycle, noting that "new technologies increase the risks that court information might be used for improper purposes such as commercial data mining, identity theft, stalking, *harassment and discrimination*".[194] It recommended, among other things, that courts "prohibit the inclusion of unnecessary personal data identifiers and other personal information in the court record" and that judges avoid disclosure of personal data identifiers and limit disclosure of personal information in their judgments.[195] It also recommended that judgments be made available online, but that steps be taken to prevent indexing and cache storage by online bots, so as to avoid searchability on general search engines like Google.[196]

The privacy/vulnerability cycle and the special concerns it raises for members of equality-seeking communities in the context of online court records is sometimes explicitly, but more often implicitly, recognized in Canadian case law, legislation, court and tribunal rules and procedures, as well as in commentary from privacy commissioners and policy makers. While explicit reference to the cycle is more likely to surface in the context of specific vulnerable populations, including young people and sexual assault complainants (who are disproportionately likely to be women),

191. *Ibid*.
192. Dickson, *supra* note 184.
193. Canadian Judicial Council, "Model Policy for Access to Court Records in Canada" (Ottawa: Judges Technology Advisory Committee, 2005), online: CJC <https://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_AccessPolicy_2005_en.pdf>.
194. *Ibid* at iii, vii [emphasis added].
195. *Ibid*, ss 2.1, 2.3.
196. *Ibid*, s 4.6.1.

it is occasionally also implicitly recognized in practices of anonymization in relation to decision making about members of other equality-seeking communities. These existing, albeit limited, acknowledgments of the privacy/vulnerability cycle, combined with concerns about widespread online dissemination and increasingly sophisticated data profiling techniques, provide a foundation and context ripe for reflecting on the relationship between privacy and equality and for developing effective measures to intervene in the privacy/vulnerability cycle.

IV. Conclusion

Although privacy at law has been abused by members of privileged groups to the disadvantage of less privileged groups, privacy, properly conceived, can also be intimately connected to autonomy, self-determination and collective social rights and values, like equality.[197] As Calo has argued, members of marginalized communities are often accorded less privacy and subjected to greater surveillance, which in turn exacerbates their exposure to further discrimination and marginalization.[198] The justice system frequently contributes to this "vicious cycle", through the over-representation of members of marginalized communities in court proceedings either against their will or in order to contest or seek redress for the results of their marginalization. It need not, however, perpetuate the "vicious cycle" of privacy and vulnerability when it comes to public access to court records. This has been recognized (albeit to a very limited degree) in the context of certain vulnerable groups, particularly children and sexual assault complainants, as well as in other privacy-based limits imposed in relation to litigation. And it need not, and should not, perpetuate that "vicious cycle" in the context of *online* public access to court records.

Calo, in the epigraph, suggests that stronger protections for the

197. See Jane Bailey, "Towards an Equality-Enhancing Conception of Privacy" (2008) 31:2 Dalhousie Law Journal 267.

198. For further discussion of the surveillance/discrimination cycle in relation to marginalized populations, see Rachel E Dubrofsky & Shoshana Amielle Magnet, *Feminist Surveillance Studies* (Durham, NC: Duke University Press, 2015).

chronically vulnerable may be in order. While we agree with the logic and moral appeal of this argument, specifying restrictions on online access to court records for chronically vulnerable communities raises at least three problems. First, identification of the "chronically vulnerable" seems to necessitate creation of hierarchies of vulnerability that, in light of the multiplicity of matrices of domination at play in the world,[199] may neither be equality-enhancing or possible to do. Second, the identification process would have to be an ongoing one as the sources and grounds and intersections of vulnerability due to social location shift and reshape themselves. This would inevitably seem to leave certain marginalized communities vulnerable and exposed until such time as their plight was recognized by the courts and incorporated into some form of privacy-protective, equality-enhancing measure. Third, as MacDonnell has pointed out, automatic "protections" for certain marginalized groups could serve to reinforce the stereotypes and discrimination against which they are intended to push back[200] by uniquely depriving members of those groups the autonomy to determine whether they wish to conceal that information about themselves.

For these reasons, and recognizing that there is no perfect solution, we return to the recommendation we put forward as a result of a prior analysis that specifically focused on the privacy issues relating to online public access to unredacted court records.[201] There we proposed maintaining public access to court records in its current form (and subject to whatever limitations laws that rein in the open court principle allow), while "introducing appropriate 'friction' in the process of accessing court records" online.[202] This could include redacting personal information from court records (including anonymizing judgments) before they are made accessible online, restricting search visibility and protecting access

199. See Patricia Hill Collins & Sirma Bilge, *Intersectionality* (Cambridge: Polity Press, 2016).
200. MacDonnell, *supra* note 2 at 144.
201. Bailey & Burkell, *supra* note 2.
202. *Ibid* at 182.

to documents.[203]

We recognize that this response goes further than necessary to intervene specifically on the privacy/vulnerability cycle because it provides a level of obscurity for both those who are members of equality-seeking groups and those who are not. However, it offers two attractive outcomes. First, it does not presume that members of certain marginalized communities *must* want to conceal information about themselves because it is *necessarily* stigmatizing or something to be ashamed of. Instead it assumes that a certain level of concealment is important to the dignity of *all* persons in the context of easy and widespread access to digital records. Second, in making that assumption, it removes the costly onus of bringing a motion to displace a presumption of openness in a proceeding from the shoulders of a party seeking privacy protection. This aspect of our proposed response could be of particular benefit to individuals from marginalized communities who are unaware of the possibility of seeking such protections and/or who are not in a financial position to press for them before a court or tribunal.

203. *Ibid* at 181, referring to Woodrow Hartzog & Frederic D Stutzman, "Obscurity by Design" (2013) 88:2 Washington Law Review 385.

Privacy by Design by Regulation: The Case Study of Ontario

Avner Levin*

This article presents the findings of a case study examining the role of the regulator in facilitating Privacy by Design ("PbD") solutions. With the introduction of PbD into the new European Union General Data Protection Regulation, *it is important to understand the conditions under which PbD can succeed and the role which regulators can play (if at all) in promoting such success. Two initiatives with similar technology are examined: first, a PbD success, the introduction of facial recognition technology into existing cameras in casinos in Ontario, and second, a PbD failure, the expanded deployment of cameras within the public transit system of Toronto. The findings are organized into three overarching themes: PbD-focused findings, leadership and organizational findings, and regulator-focused findings. The article argues that privacy continues to persist as an engineering problem despite PbD, that (related to that) there is growing recognition of privacy as an issue of organizational change and leadership, and consequently, that the role of the regulator must evolve if PbD is to become a meaningful regulatory tool, an evolution that carries with it both risks and opportunities for privacy.*

* Professor, Law & Business Department, Ted Rogers School of Management, Ryerson University. This paper was supported by a research grant from the Blavtanik Interdisciplinary Cyber Research Center, Tel Aviv University. Many thanks to Professor Michael Birnhack of the Buchmann Faculty of Law, Tel Aviv University for leading this research project and for the fruitful discussions we had on privacy by design and to Michelle Chibba of the Privacy & Big Data Research Institute at Ryerson University for her invaluable research support and her contribution to the many drafts of this paper.

I. Introduction
II. Privacy by Design
III. The Case Study
  A. The Legal and Regulatory Background
  B. The Two Initiatives
    1. The Toronto Transit Commission ("TTC")
    2. The Ontario Lottery and Gaming Commission ("OLG")
    3. The TTC Initiative
    4. The OLG Initiative
  C. Research Methodology
IV. Findings
  A. The PbD Theme
    1. PbD and Legacy Systems
    2. Initial Reaction to PbD
    3. Working with PbD Principles
    4. PbD and Education
    5. Legislating PbD
    6. Theme Summary
  B. The Organizational Theme
    1. Internal Support
    2. The Role of the Internal Privacy Office
    3. Theme Summary
  C. The Regulator Theme
    1. The Regulator's Role in Early Stages
    2. Regulatory Support for the Initiatives
    3. Primary vs Secondary Regulator
    4. Collaboration or Enforcement
    5. The Overall Role of the Regulator
    6. Theme Summary
V. Conclusions
  A. Privacy as an Engineering Problem
  B. Privacy, Organizational Change, and Leadership
  C. PbD as a Regulatory Tool
  D. The Future of PbD

I. Introduction

This paper presents the findings of a case study examining the role of the regulator in facilitating Privacy by Design solutions. PbD is an approach to privacy which urges organizations to design privacy into new initiatives rather than deal with privacy as an after-the-fact "problem". The approach has been embraced by many, but executed by few, for a number of reasons, such as the difficulty in translating the idea of PbD into engineering algorithms. With the introduction of PbD into the new European Union *General Data Protection Regulation*[1] ("*GDPR*"), it is important to understand the conditions under which PbD can succeed, and the role regulators can play (if at all) in promoting such success.

This case study contributes to this understanding by examining the Province of Ontario, Canada, and the role of its Information and Privacy Commissioner in two PbD initiatives. Ontario was not chosen at random. Its Privacy Commissioner at the time the initiatives were taking place, Dr. Ann Cavoukian, was a champion of PbD. Cavoukian tirelessly and passionately promoted PbD both domestically and internationally, and outcomes such as the 2010 Jerusalem Declaration of Privacy Commissioners in support of PbD and the inclusion of PbD in the new *GDPR* can largely be attributed to her advocacy.

This case study wishes to examine the role the Commissioner played as a regulator and whether the conduct of the regulator had any bearing on the success or failure of PbD. The two initiatives that are examined are the introduction of facial recognition technology into existing cameras in casinos in Ontario, an initiative that is generally lauded for the success of PbD, and the expanded deployment of cameras within the public transit system of Toronto, in which PbD did not take hold. Since, in both instances, the potentially intrusive technology and its potential PbD solution were similar, the case study is able to focus on the role of

1. EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1, art 25(1) [*GDPR*].

the regulator and the regulator's impact with greater certainty.

The paper is divided into the following sections. After this first introductory section, it discusses and introduces PbD, its principles, and its evolution, leading in the second section to its incorporation into regulatory frameworks. The second section also reviews engineering challenges to the application of PbD and other relevant criticisms of PbD. The third section provides the methodology and the details of the case study and how the interviews conducted during the case study were analyzed to arrive at the findings of this paper. The fourth section then sets out the findings. Finally, the fifth section draws conclusions from the findings in three main areas: the persistence of privacy as an engineering problem, the growing recognition of privacy as an issue of organizational change and leadership, and consequently, the evolution of the role of the regulator with some thoughts as to how PbD can best flourish when it is part of a regulatory framework.

II. Privacy by Design

The origin of PbD can be found in early efforts to take the intent of the Fair Information Practice Principles ("FIPPs") and translate these principles into the design and operation of information and communication technologies.[2] The concept of Privacy-Enhancing Technologies ("PETs"), as this effort was then known, showed how FIPPs could be reflected in information and communication technologies to achieve strong privacy protection. However, where PETs focused on technology and its potential to protect privacy, PbD prescribed that privacy be built directly and holistically into the design and operation, not only of technology, but also of operations, systems, work processes, management structures, physical spaces, and networked infrastructure. In this sense, PbD was the

2. For an extended treatment of PbD origins, see Ann Cavoukian, "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era" in George OM Yee, ed, *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (Hershey, PA: IGI Global, 2011) 170; Ann Cavoukian, "Privacy by Design: Leadership, Methods, and Results" in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (New York: Springer, 2013) 175.

next step in the evolution of the privacy dialogue that first led to PETs.[3]

As formulated by Cavoukian, PbD consists of a set of seven "foundational principles". These are:

1. Proactive, not Reactive; Preventative, not Remedial
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy[4]

At the time of its initial formulation (the early 1990s), PbD represented a significant shift from traditional approaches to protecting privacy, which focussed on regulation by setting minimum standards for information management practices and providing remedies through legal and regulatory instruments for privacy breaches. The traditional regulatory approach was described by Alexander Dix (former Berlin Commissioner for Data Protection and Freedom of Information) as "[l]ocking the stable door after the horse has bolted".[5] In contrast, PbD allowed for greater regulatory flexibility:

> In the past, FIPPs have largely been discharged through the adoption of policies and processes within the firm: privacy has been the bailiwick of lawyers. Now, under the rubric of "privacy by design," policymakers are calling on the private sector to use the distinct attributes of code to harden privacy's protection.[6]

---

3. See *e.g.* Gerrit Hornung, "Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework" (2013) 26:1–2 Innovation: The European Journal of Social Science Research 181 (some still appear to conflate PbD with PETs).
4. Information and Privacy Commissioner, Ontario, Canada, "Privacy by Design: The 7 Foundational Principles", by Ann Cavoukian (Toronto: IPC, August 2009).
5. Alexander Dix, "Built-in Privacy—No Panacea, But a Necessary Condition for Effective Privacy Protection" (2010) 3:2 Identity in the Information Society 257 at 257.
6. Deirdre K Mulligan & Jennifer King, "Bridging the Gap Between Privacy and Design" (2012) 14:4 University of Pennsylvania Journal of Constitutional Law 989 at 992 [Mulligan & King, "Bridging the Gap"].

Since its original formulation by Cavoukian, PbD has steadily gained recognition and acceptance over the last two decades, and while it seemed radical at first, it has come into widespread usage as part of the vocabulary of privacy regulators, advocates, and information technology professionals as well as the subject of flattering media articles.[7] A major milestone in this journey was the Jerusalem 2010 resolution of the International Privacy and Data Protection Commissioners.[8] The resolution recognized PbD as an "essential component of fundamental privacy protection".[9] The resolution further "[encourages] the adoption of Privacy by Design's Foundational Principles" as part of "an organization's default mode of operation"[10] and "[invites] Data Protection and Privacy Commissioners/ Authorities to: promote Privacy by Design …; foster the incorporation of [its] Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions …; [and] encourage research on Privacy by Design".[11]

Indeed, research into PbD has flourished following the resolution. From specific projects attempting to demonstrate the success of particular

7. Kashmir Hill, "Why 'Privacy By Design' Is The New Corporate Hotness" *Forbes* (28 July 2011), online: Forbes <https://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/>.
8. 32nd International Conference of Data Protection and Privacy Commissioners, "Resolution on Privacy by Design" *International Conference of Data Protection and Privacy Commissioners* (29 October 2010), online: ICDPPC <www.icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>.
9. *Ibid* at 2.
10. *Ibid*.
11. *Ibid*.

approaches, such as facial recognition,[12] ubiquitous computing,[13] internet protocols,[14] and other "privacy-invasive technologies"[15] to more general attempts to apply PbD to information and communication technologies,[16] to projects that argue that PbD implementation should be based on an understanding of contemporary privacy practices,[17] the cumulative effect of academic research into PbD has been largely to assist in the ongoing transformation of PbD from a theoretical concept into a regulatory instrument.[18] In 2014, Australia's Commissioner referred to PbD explicitly in its guidelines to Australia's new privacy legislation,[19] and Victoria became the first Australian state privacy office to explicitly

12. Juanita Pedraza et al, "Privacy-by-design rules in face recognition system" (2013) 109:1 Neurocomputing 49.
13. Marc Langheinrich, "Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems" in Gregory D Abowd, Barry Brumitt & Steven Shafer, eds, *Ubicomp 2001: Ubiquitous Computing: International Conference Atlanta, Georgia, USA, September 30–October 2, 2001 Proceedings* (New York: Springer, 2001) 273.
14. Adamantia Rachovitsa, "Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue" (2016) 24:4 International Journal of Law and Information 374.
15. Demetrius Klitou, *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century* (The Hague: TMC Asser Press, 2014).
16. Marc van Lieshout et al, "Privacy by Design: An Alternative to Existing Practice in Safeguarding Privacy" (2011) 13:6 Info 55; Dag Wiese Schartum, "Making Privacy by Design Operative" (2016) 24:2 International Journal of Law and Information Technology 151.
17. Kenneth A Bamberger & Deirdre K Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, MA: MIT Press, 2015).
18. Mulligan & King, "Bridging the Gap", *supra* note 6; Ira S Rubinstein, "Regulating Privacy by Design" (2011) 26:3 Berkeley Technology Law Journal 1409.
19. Tarryn Ryan & Veronica Scott, "AUSTRAILIA — Australia Legislates for Privacy by Design" *International Association of Privacy Professionals* (11 February 2014), online: IAPP <https://iapp.org/news/a/australia-australia-legislates-for-privacy-by-design/>.

endorse and implement PbD.[20] In the United States, the proposed *Commercial Privacy Bill of Rights Act of 2015* referenced PbD explicitly and would have required it as a business practice.[21] The Congressional Privacy Bill directly followed the release of the White House's proposal for a privacy bill, which also mentioned PbD, suggesting that the US government had a clear policy of incorporating PbD principles into its legislative initiatives.[22]

In Europe, the European Commission ratified the final version of the *GDPR* in 2016.[23] The Regulation will be enforced beginning in 2018, providing organizations with two years to become compliant. Article 25 of the *GDPR* codifies both the concepts of PbD and privacy by default.[24] Under this Article, an organization ("data controller") is required to implement appropriate technical and organizational measures both at the time of determination of the means for processing and at the time of the processing itself in order to ensure that data protection principles are met. In addition, the organization will need to ensure that, by default, only personal information which is necessary for each specific purpose of the data processing is, in fact, processed. Personal information will not be automatically made available to third parties. Social media companies, for example, will no longer be able to offer default settings for their apps in which information is shared or available to the public.

---

20. Hamish Barwik, "Victoria to adopt Privacy by Design: Victorian Commissioner" *Computerworld* (6 May 2014), online: Computerworld <www.computerworld.com.au/article/544416/victoria_adopt_privacy_by_design_victorian_commissioner>; Commissioner for Privacy and Data Protection, "Privacy by Design: How to manage privacy effectively in the Victorian public sector" (20 November 2014), online: CPDP <www.cpdp.vic.gov.au/images/content/pdf/CPDP_Media_Release_Privacy_by_Design_20_November_2014.pdf >.
21. HR 1053, 114th Cong, s 113.
22. Libbie Canter, "White House Privacy Bill: A Deeper Dive" *Inside Privacy* (27 February 2015), online: Inside Privacy <https://www.insideprivacy.com/advertising-marketing/white-house-privacy-bill-a-deeper-dive/>.
23. *GDPR*, *supra* note 1.
24. EC, *Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market* (Brussels: 28 January 2015).

The explicit incorporation of PbD for the first time into a major legislative initiative has placed both the concept and the manner in which it has been incorporated into the *GDPR* under intense scrutiny. Some have hailed the *GDPR* for taking a "flexible approach" to PbD.[25] Organizations implementing PbD, for example, will be able to take into account costs as well as conduct a risk assessment in order to determine the appropriate level of privacy protection and design. Others, however, have criticized the European approach for being too focussed on the notion of privacy as control over personal information, which is a notion favoured by information and privacy commissioners.[26] Mainly, however, questions remain as to how PbD will actually be applied as part of the *GDPR*. How will this norm be understood and enforced? Some attempt to bridge the gap between law and engineering,[27] while others believe it is difficult, if not impossible to bridge this gap, and accordingly see the application of PbD to other dimensions of organizational behaviour.[28]

The purpose of this paper is to contribute to the debate over the success of and future application of PbD through the examination of two initiatives in Ontario using the case study method. The case study method has been used by others with respect to PbD, but somewhat

25. Frederick Leentfaar, "Privacy by design and default" *Taylor Wessing* (November 2016), online: Taylor Wessing <https://www.taylorwessing.com/globaldatahub/article-privacy-by-design-and-default.html>.
26. Deirdre K Mulligan & Kenneth A Bamberger, "What Regulators Can Do to Advance Privacy Through Design" (2013) 56:11 Communications of the ACM 20.
27. Michael Colesky, Jaap-Henk Hoepman & Christiaan Hillen, "A Critical Analysis of Privacy Design Strategies" (Paper delivered at the 2016 IEEE Security and Privacy Workshops in San Jose California, 26 May 2016), Security and Privacy Workshops, 2016 IEEE 33.
28. Bert-Jaap Koops & Ronald Leenes, "Privacy Regulation Cannot be Hardcoded: A Critical Comment on the Privacy by Design Provision in Data-Protection Law" (2014) 28:2 International Review of Law, Computers & Technology 159; see also Michael Birnhack, Eran Toch & Irit Hadar, "Privacy Mindset, Technological Mindset" (2014) 55:1 Jurimetrics 55.

tangentially.[29] In contrast, this paper centres on two initiatives in which potentially intrusive technology was introduced with explicit references to PbD and the findings that can be drawn from them in order to determine the role of regulatory intervention and contribute to the conversation as to how PbD may be applied when it is set as a legal standard. The following section discusses the details of the initiatives and the case-study methodology used in their exploration.

III. The Case Study

A. The Legal and Regulatory Background

The Province of Ontario (Canada) has specific privacy legislation for organizations operating in the public sector. The *Freedom of Information and Protection of Privacy Act*[30] ("*FIPPA*") and the *Municipal Freedom of Information and Protection of Privacy Act*[31] ("*MFIPPA*") govern the public sector at the provincial and municipal levels, respectively. However, Ontario has no specific privacy legislation for organizations operating in the private sector. Instead, the federal *Personal Information Protection and Electronic Documents Act*[32] ("*PIPEDA*") applies to the private sector. Ontario also has specific privacy legislation for health service providers, the *Personal Health Information Protection Act*[33] ("*PHIPA*"). Private sector operators in the health sector are governed by *PHIPA* as well, which is considered substantially similar to *PIPEDA*.

The Information and Privacy Commissioner of Ontario ("IPC") is the regulator that enforces *FIPPA*, *MFIPPA*, and *PHIPA*. The Commissioner

29. Inga Kroener & David Wright, "A Strategy for Operationalizing Privacy by Design" (2014) 30:5 Information Society 355.
30. *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31 [*FIPPA*].
31. *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56 [*MFIPPA*].
32. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
33. *Personal Health Information Protection Act*, SO 2004, c 3, Schedule A [*PHIPA*].

is appointed by and reports to the Legislative Assembly of Ontario and is independent of the executive branch. Under the three acts and statutory mandate, the Commissioner is responsible for:

- Resolving access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction;
- Investigating privacy complaints with respect to personal information held by government or health care practitioners and organizations;
- Ensuring that the government organizations and health information custodians comply with the provisions of the Acts;
- Educating the public about Ontario's access and privacy laws; and
- Conducting research on access and privacy issues and providing advice and comment on proposed government legislation and programs.[34]

During Cavoukian's fifteen-year tenure as Commissioner, her office carried out its mandate under what became known as the "3C" approach — Consultation, Co-operation, and Collaboration. Co-operation was emphasized over confrontation to resolve complaints. Collaboration was sought proactively by seeking partnerships to find joint solutions to emerging privacy and access issues.[35] Internally, her 3C approach led Cavoukian to create a research, policy, and special projects department that was separate and distinct from the Office's compliance, enforcement, investigations, and complaints responsibilities. This department had a

34. Information and Privacy Commissioner of Ontario, "Role and Mandate", online: IPC <www.ipc.on.ca/about-us/role-and-mandate/>.

35. This approach led, for example, to positive results in the area of privacy breaches. Public institutions covered under *FIPPA* and *MFIPPA* voluntarily self-reported data breaches to the IPC despite the *Acts* having no breach notification requirements. Hundreds of data breaches were reported voluntarily in this way, allowing the office to play a vital role at critical breach management stages.

diverse set of skills and competency with a focus on policy, legal, and technology expertise and played a significant role with respect to the two initiatives discussed here.

B. The Two Initiatives

The focus of this paper is on two organizations that are covered by Ontario's privacy legislation and for which the IPC has oversight responsibilities. Brief background information on each of the institutions is provided below.

1. The Toronto Transit Commission ("TTC")

The TTC is an agency of the City of Toronto and is overseen by a Board.[36] The TTC is responsible for public transit within the municipal area of Toronto by means of busses, streetcars, and subway trains. The TTC is regulated by the IPC under *MFIPPA*, but unlike the Ontario Lottery and Gaming Corporation ("OLG") (discussed below), there is no formal regulator that provides oversight for the core activity of the TTC (transportation). The TTC is governed by general legislation applicable to other public sector agencies and by the City of Toronto by-laws.

2. The Ontario Lottery and Gaming Corporation ("OLG")

The OLG is an "Operational Enterprise Agency" of Ontario. Its purpose is to provide gaming and lottery entertainment (casinos, lotteries, horse-racing etc.) while maximizing benefits in a "socially responsible manner".[37] As an operational enterprise agency, the OLG has a single shareholder, the Government of Ontario, and it reports through its Board of Directors to Ontario's Minister of Finance. Board appointments are not full-time, and

---

36. Toronto Transit Commission, "The Board" *Toronto Transit Commission*, online: TTC <www.ttc.ca/About_the_TTC/Commission_reports_and_information/index.jsp>.
37. Ontario Lottery and Gaming Corporation, "ABOUT OLG" *Ontario Lottery and Gaming Corporation*, online: OLG <about.olg.ca/who-we-are/>.

Directors do not manage the OLG directly.[38] The OLG is an institution governed by *FIPPA*, but its main regulator, for the purposes of gaming, is the Alcohol and Gaming Commission of Ontario[39] ("AGCO"). The AGCO operates under the *Alcohol and Gaming Regulation and Public Protection Act*, 1996.[40] Unlike the IPC, the AGCO is not independent of the government and reports to the Ministry of the Attorney General.[41]

3. The TTC Initiative

The TTC initiative began with a complaint to the IPC in the fall of 2007. Privacy International, an organization based in England, complained about the TTC's plan to expand its CCTV surveillance systems by adding more video surveillance cameras in the subway system. It is noteworthy to mention that the TTC already had in place a robust CCTV surveillance program (with policies and procedures) and an extensive systems network that included older analog and newer digital CCTV technology.[42] According to the letter, the TTC was in violation of *MFIPPA*.[43] The IPC launched an investigation into the TTC's practices in response to the letter of complaint. The investigation did not proceed in a traditional manner given the heightened public interest in video surveillance systems at the time and the impact of these systems on privacy. Cavoukian decided that alongside the formal investigation of the complaint, her office would expand the investigation to examine "the role that privacy-enhancing technologies can play in mitigating the privacy-

38. Ontario Lottery and Gaming Corporation, "Our Reporting Structure" *Ontario Lottery and Gaming Corporation*, online: OLG <about.olg.ca/corporate-governance/>.
39. Alcohol and Gaming Commission of Ontario, online: AGCO <www.agco.on.ca/en/whatwedo/index_commercial.aspx> [AGCO].
40. *Alcohol and Gaming Regulation and Public Protection Act*, SO 1996, c 26, Schedule.
41. AGCO, *supra* note 39.
42. Information and Privacy Commissioner of Ontario, "Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report", by Ann Cavoukian, Privacy Investigation Report MC07-68 (Toronto: IPC, 3 March 2008) at 16 [IPCO, "Privacy and Video Surveillance"].
43. *Ibid*.

invasive nature of video surveillance cameras".[44] In the introduction to the section of the report discussing PETs, Cavoukian further stated: "it is essential that privacy protections be built directly into [the] design and implementation [of technology], right from the outset. This view is captured in my mantra of 'privacy by design'".[45] The report then discussed a specific form of image and object detection and encryption developed by research engineers at the University of Toronto ("U of T").[46]

The investigative report found that the TTC was in compliance with *MFIPPA*.[47] Still, the report outlined twelve recommendations for the TTC of which two related to the software solution and PbD:

> 11. That the TTC should keep abreast of research on emerging privacy-enhancing technologies and adopt these technologies, whenever possible.
>
> 12. That the TTC should select a location to evaluate the privacy-enhancing video surveillance technology developed by the University of Toronto researchers[48]

The final recommendation required the TTC to provide "proof of compliance or an update on the status of its compliance with each of the recommendations" within three months of the date of the Report.[49] Unlike other investigation reports often handled exclusively by the Office's compliance, enforcement, investigations, and complaints unit, the research, policy, and special projects department was brought in to collaborate with the TTC on this technology recommendation.

The exploration by the TTC of privacy-enhancing video surveillance was a direct result of the recommendation to do so by the regulator in the investigation report. The TTC responded by providing the U of

---

44. *Ibid* at 1.
45. *Ibid* at 12.
46. Karl Martin & Konstantinos N Plataniotis, "Secure Visual Object Based Coding for Privacy Protected Surveillance" (2007), Draft Submitted to IEEE Transactions on Circuits and Systems for Video Technology, online: IEEE <www.comm.toronto.edu/~kostas/Publications2008/pub/submitted/2007-submitted-Martin-ieee_csvt_secure_stspiht.pdf>.
47. IPCO, "Privacy and Video Surveillance", *supra* note 42 at 43.
48. *Ibid* at 44.
49. *Ibid*.

T researchers access to a test environment and its subway monitoring room to allow the researchers to evaluate the feasibility of the technology in a subway platform context over a few months. After the researchers completed the testing and evaluation of the technology, the TTC determined that it would not be possible to incorporate the software technology into its CCTV systems.

4. The OLG Initiative

Unlike the TTC initiative, the OLG Privacy by Design project did not arise out of an official complaint and investigation report. Instead, also in 2007, the OLG approached the IPC to discuss whether it would be legally permissible for the OLG to adopt facial recognition technology for its voluntary "self-exclusion" program. The "self-exclusion" program allows persons that are addicted to gambling to ask the OLG to remove them from gambling premises that they wish to enter. The approach used until then by the OLG was paper-based, requiring security officers to review photos and related identification information on the program registrants and then manually attempt to recognize registrants and pick them out of the casino crowds.[50] The OLG sought to modernize its monitoring of individuals entering gambling facilities after several incidents in which individuals were not recognized and, therefore, not removed from gambling facilities even though they were enrolled in the "self-exclusion" program.

The result of the preliminary discussion was a research and pilot project into the development and application of biometric encryption to the OLG's facial recognition system. The project required collaboration between the OLG, the IPC, the U of T, and iView (a video surveillance vendor). The IPC's research policy and special projects department led this initiative, with no involvement from the enforcement, compliance, investigations, and complaints sections of the IPC.

---

50. For more information on the operation of OLG's self-excluded program see: Information and Privacy Commissioner, Ontario, Canada, "Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept", by Ann Cavoukian & Tom Marinelli (Toronto: IPC, November 2010) [IPCO, "Privacy-Protective Facial Recognition"].

At the end of the project, the OLG successfully implemented the technology in twenty-seven of its locations.[51] The IPC and the OLG also published a report in which they reported on the success of the project and the successful integration of the technology developed at the U of T with the OLG's facial recognition system: "This use of BE as a secondary classifier was shown to enhance patron privacy (both for those on the watch list, and regular patrons), system security, and even overall accuracy of the watch list system within the context of the OLG self-exclusion program".[52]

C. Research Methodology

This research project used a case study approach to examine the introduction of PbD into the OLG and the TTC's response to embedding privacy into video surveillance technology and the role that the regulator had in these organizations taking a PbD approach. Semi-structured interviews were conducted with at least three individuals involved in each initiative who had an active and leadership role from both a strategic policy and technical perspective. The questionnaire is included as an appendix to this paper. The interviews were recorded, transcribed, and then read by members of the research team to identify key threads in the conversations and arrive at the findings listed in the following section. It should be noted that individuals were asked to recollect details on an initiative in which they were involved ten years ago and that, as is with any case study, the ability to generalize from it is limited.

Participants are not identified and referred to in the project, and quotations from their interview, according to the table below, include brief, non-identifying information about each participant:

Participant	Role
P1	Strategic decision-maker

51. Sharon Oosthoek, "OLG facial scans to help gambling addicts" *CBC News* (26 November 2010), online: CBC <www.cbc.ca/news/technology/olg-facial-scans-to-help-gambling-addicts-1.929760>.
52. IPCO, "Privacy-Protective Facial Recognition", *supra* note 50 at 14.

P2	Senior project management/ technical
P3	Legal/regulatory
P4	Project implementation/senior technical
P5	Project implementation
P6	Legal/regulatory
P7	Research/technical

IV. Findings

It is worth repeating the cautionary methodological note about generalizing from this case study of PbD in Ontario, Canada to the success or failure of PbD in other jurisdictions. With that caveat in mind, this section presents the main points about the implementation of PbD and the role of the regulator that emerges from the interviews. The findings are organized into three overarching themes. The first theme focuses on PbD — reaction to the concept, working with the principles, engineering challenges, etc. The second theme centers on the organizational and leadership dimensions of the two initiatives. Finally, the third group consists of those findings that focused on the regulator — the ideal regulatory role, the place of legislation, the support given by Cavoukian's office, etc.

A. The PbD Theme

1. PbD and Legacy Systems

The constraint of existing technological and infrastructure systems — "Legacy Systems" is both a conceptual and practical barrier to the implementation of PbD:

> Privacy by design presupposes … a process whereby a new information system is designed or an existing system is redesigned or adjusted. Building systems from scratch opens for more possibilities than does changing existing systems. Comprehensive changes in existing systems will often meet some clear limitations: Basic properties of information systems greatly limit

> improvements.[53]

Such a constraint existed both at the OLG and at the TTC. Yet the search for a privacy-protective solution created an opportunity since there were no "off-the-shelf" solutions for the facial recognition problems that both organizations faced. P2 stated:

> When we talked about using facial recognition, a lot of people said, well that's been tried before, you're going to waste your time. And I would give [to P1] who was the person that said we're going to do this, at the start. Which kind of put the gauntlet out to the technology people – now we've got to step up and see if we can do this.

And P5 added:

> "it was always we were going to be doing biometric encryption with facial recognition to protect privacy". That is of course, in a sense, a precondition for the idea of PbD to begin with. Choosing to design privacy into a solution may have been easier, therefore, because a solution had to be developed "from scratch".

While at the OLG, the search was on for a specific privacy-protective solution to the problem of self-excluded patrons seeking re-entry. At the TTC it appears that the scope was wider. The TTC already had a network of CCTV cameras that were used in the subway, some of which belonged to a legacy system (*e.g.* analog cameras). As noted by P7:

> This system was the existing one including existing cameras and storage/monitoring infrastructure for buses, streetcars and subway station platforms. In other words, this project was looking at [the] existing legacy system – it was not about designing a new system. It was retrofitting. Two options were available: i) put in a new system; or ii) retrofit the existing system to comply with PbD.

The TTC also had to deal with separate policy concerns, ranging from passenger safety and operator safety to national security concerns post 9/11.[54] It seems that it was easier to design and apply an innovative solution to a limited problem than it was to retrofit an existing legacy system meant to address a wide range of policy concerns.

---

53. Schartum, *supra* note 16 at 161; see also Nigel Davies & Marc Langheinrich, "Privacy by Design" (2013) 12:2 IEEE Pervasive Computing 2 [Davies & Langheinrich, "Privacy by Design"].
54. P6, transcript on file.

2. Initial Reaction to PbD

It appears that the OLG staff were not specifically aware of PbD as an idea or of its principles. Staff at different levels reacted to PbD differently. P1 saw the public policy appeal:

> It always starts with an idea of design, if you build in that planning and thoughtfulness at the front end of work, that privacy and protection of information is not something that happens at the end of the story, it happens all the way through and why is that different, than anything else we would design?

But for P2, PbD initially held little value:

> To be honest when I first read the principle I thought so how [is] this going to help us … because it's so conceptual … how are we going to take these principles and actually get down to doing facial recognition to aid in self-exclusion. I would tell you that the technical guys were not convinced that we could do this.

P5 was also lukewarm:

> I thought, well it doesn't really make a lot of sense actually. That's really what I thought. Well my initial thoughts were, I don't see, I don't understand this. Because I'm looking at it purely from a solution point of view. It really was difficult for me at the beginning to understand, why we were putting biometric encryption in. The reason I had a big issue with it, was because what we were calling the biometric, the image, was already public. So it was already out there, and it actually had to be out there in order for the security officers to be able to identify people. So we could not actually hold that secret. We couldn't do it. So it had to be, it actually had to be open, and I'm saying, well if it's already open, then what is biometric encryption doing here.

At the TTC, there were similar concerns about the conflation of PbD with biometric encryption and whether there was any advantage to the U of T research project over existing commercial solutions. Explains P6:

> I don't think that there were any issues with the privacy by design, there were suggestions or recommendations that you go look at technology that U of T was studying. So you were kind of led down a specific kind of path from a privacy by design perspective, and I will tell you the engineers didn't necessarily think what [U of T] had was so different than what already existed in the market.

Against such mixed reaction, it seems that the regulator's role was crucial in both convincing and supporting the OLG in its attempt to design privacy rather than focus on "merely" being in compliance.

3. Working with PbD principles

For the OLG initiative, the search for a solution that would allow for biometric facial recognition and protect the privacy of customers captured in the system evolved and transformed over time. P4 said that initially: "[the Commissioner's] thinking was kind of an interesting concept, in terms of being able to protect biometric in the database, and that was the problem we were trying to solve". However, it seems that the early attempts were not successful. P5 commented on the lack of familiarity with PbD and its principles:

> I didn't have a lot of privacy by design experience … So maybe a few months in, or six months in we started to look at the privacy by design principles, and what I did was an alignment exercise to say, how do we align? You know the stuff that we're planning on doing and going to be doing. How does that align to the seven principles? My question in terms of trying to go through the design process and the solution process is, are those principles there to sort of have you wrestle with them as you try and come up with these solutions and have the conversation with the commissioner, or is that something that you're sort of already advanced in terms of the solution and then you sort of tried to fit what you were doing to these ideas of privacy by design?

Following the alignment exercise, P5 described the process of searching for a privacy solution and how the "problem" was re-defined: "I had an idea of how we could use biometric encryption that I could live with … So I had a conversation in one of our meetings … and the first thing [the Commissioner] said was that's an absolutely good use of biometric encryption". After the approval of the Commissioner for the new manner in which privacy was to be designed into the facial recognition system, P5 concluded: "A lot of weight came off me, because now I could believe in it, and I could actually build something that makes sense".

P4 also shared concerns over the technology of biometric encryption and whether it was compatible with PbD principles, specifically the "full functionality" principle: "That's what the research was all about, if it wasn't going to work, one of the things we would stop, the whole concept of biometric encryption because it wasn't going to be feasible". And more generally P4 added:

> Do I believe that we were on the right page on protecting people's privacy from day one? I think we were, but because we look at the holistic solution around privacy, I think the risk, when you look at the necessity for biometric

> encryption, it's not clear that we had to do that. So I think as a case study, there were some good benefits out of it, but at the end of the day, privacy by design and the principles of privacy by design, are good software engineering design principles regardless. How practical each one of them are, are totally dependable on each individual project.

In addition, the OLG was concerned with fundamental privacy principles such as Purpose Specification and whether their proposal to digitize and store facial images would comply with it. P3 pointed out that:

> What we have to guard against, is having their image … on file so that it could potentially be used for a secondary purpose, if there's a crime in the area and the police come to you, with a warrant, with a lawful court order, and they say we want to access all your biometric that you have on file … that would be a secondary use that even though it is lawful … we wouldn't want that.

P4 also noted that there were other, more protective alternatives that were less attractive from a commercial point of view: "OK Ontario, basically say everybody, anyone who wants to buy a gaming product, needs to have a card, needs to be registered. Ontario doesn't want to go there, right …"

At the TTC, the project never progressed beyond the research phase, seemingly not because of difficulties related to working with PbD and its principles but because of technological obstacles. According to P7:

> The solution could be implemented but remember this was done several years back unlike the advances that have developed recently in the area of CCTV systems … If the TTC invested early on and made a commitment to this privacy enhancing technology, this encoding could be done on the camera which is more secure and easy to implement.

4. PbD and Education

Participants were asked to generalize about PbD on the basis of their experience and their specific project. P2 believes that education of engineers in PbD is absolutely essential if it is to succeed beyond a few examples:

> I think [PbD] principles are just what they are, principles. So they guide you. I think the body of knowledge has to follow after that. So I often thought about the universities, and within some of these information programs that you actually start introducing the concepts of the seven principles into the university so that the students that are coming out are very aware.

P7 added that part of the difficulty is that engineering education is

regulated and largely prescribed by the profession:

> To do [PbD] requires, needs, direction to engineers to do it. Nothing prevents this in technical solutions. It is difficult with undergraduate [education]. Engineers are regulated. It takes a bit more time for engineers to react. 10-20 years ago privacy was not so important … I don't see problems with integrating PbD into curricula or into products.

As to the PbD principles and whether they are detailed enough to provide guidance for engineers, P7 is of the opinion that "what is missing is the educated people who can take the inspirational message [of PbD] and make sense of it". For P7, that is similar to any other engineering design exercise: "customer gives specs the way the customer understands. The designer/builder needs to translate the customer specs. [We] need people to take [the privacy] message and translate it".

5. Legislating PbD

Based on the TTC project, P6 is concerned about any attempt to legislate or impose PbD: "when the organization wants something, and you do it in consultation, then the privacy by design concept gets a much bigger play, and succeeds. When imposed, it has far less opportunity to be successful".

P3 is pleased with the legislation of PbD but concerned about the bureaucratization of PbD:

> First of all here's why I think it's a very positive thing to have it in the legislation. By having it in, the *GDPR* in the statute, it automatically elevates, because companies will now be required to embed privacy as the default, to have privacy by design, data prediction by design, it's no longer just a suggestion, it's required, and that by necessity will raise the bar. You can kind of see it as default. We're talking positive consent that is not the prevailing standard as you know. So that's what raises the bar. My only concern, I don't even want to express this as a concern but a question. I don't want this to get regulated to death.

That may be because other regulators have been slow to embrace PbD, although now it enjoys regulatory consensus. According to P3:

> the whole privacy by design thing, it took three years of presentations at the EU commissioners meeting, before it took off. The first couple of years it received polite applause perhaps. The third year, the UK commissioner she came from the telco world, and then she became commissioner, and she got it like this, and then the EU has commissioner's meetings, the EU commissioners, she

> started propagating it and it just flew after 2004-5.

Therefore, it is notable that PbD has enjoyed the greatest success with regulators that have a non-legal background.

6. Theme Summary

The main findings emerging from the PbD theme, therefore, relate to the gap between the principles of PbD and the concept of PbD on the one hand and the attempts of implementing PbD as an engineering solution on the other. The constraints of having to work with legacy systems, the lack of familiarity with PbD, and its principles necessitating both a learning curve as well as time-consuming mapping exercises in which PbD is mapped against software and hardware design processes with which engineers are more familiar led to a difficult implementation process. In one initiative, this process stalled, while in the other it had to be restructured and rethought in order to arrive ultimately at a successful solution. One suggestion that would assist in bridging this gap was the educational one — the inclusion of PbD and its principles in the contemporary engineering curriculum. Notably, the move to enshrine PbD in legislation was met with concerns.

B. The Organizational Theme

1. Internal Support

Overall, internal support for the project at the OLG was achieved by ensuring that all internal stakeholders were updated. Beyond the support of leadership from a public policy perspective, the design of privacy into the facial recognition system required the support of the technical staff that worked on the project. P2 described the process:

> Our approach was pretty structured … so there was never all of a sudden somebody coming in and [raising concerns]. So at any point in time, when we went through that structure, we educated our stakeholders. We brought them in the room, sat down, and talked to them about what we found, the good the bad and the ugly, because there were a few times that we actually thought that it wasn't going to work.

At that key moment, when the OLG could have decided to stop pursuing

the design of privacy, the support of the regulator and of the technical staff was crucial. Continues P2:

> we actually had a meeting down at [the Commissioner's] office and she was quite clear that she wanted us to move forward with this, so back at the ranch we sat down and we brainstormed. How is this going to work? And I would say a key individual that we actually brought on at that time … who actually took it upon himself to say, look I'm going to try to solve this … I wasn't quite confident that we can actually pull off the design, until this gentleman came in, and he took it upon himself as a challenge.

The success of the solution beyond PbD assisted with the support for privacy in general in the organization in subsequent years. P5 explains:

> we actually came up with examples of how we were actually adhering to the PbD principles and in some cases not, right. So we looked at the one about positive sum and what that means, as an example, and then we looked at what we were doing. Here's a perfect time to tell you about the unexpected benefit of biometric encryption. We had the two classifiers, face recognition whittling down the problem, and then biometric encryption taking over. Just the fact that you're doing two different classifiers, it actually made your accuracy of the system better. What that did is it actually led people to believe in the system more, where they say, yeah we're going to get some false alarms, but we've brought it down from 4% false alarms – which is a lot, down to under 2%. Which is pretty damn good. Like in the biometric field, that's really really good results.

At the TTC, internal support never built up for the biometric encryption PbD initiative and perhaps, consequently, it did not progress beyond the research stage. Apart from the concerns over working specifically with the research team at the U of T (mentioned above), it seems the specific PbD route proposed by the Commissioner was incompatible with existing TTC technology at the time. P6 elaborated:

> If you were doing live monitoring, [the proposed solution] would help to address privacy issues about how much information people were seeing. Where there was a disconnect, [the TTC] did very little monitoring … and the places where it would be monitored, our systems are so old that even [there] they said you couldn't do it.

According to P7, the TTC did not provide funding on a comparable level to that of the OLG:

> The project lasted only a few months which included meetings. No funding from TTC. [The Commissioner] provided 'in kind' resources – staff for project management. TTC provided 'in kind' resources – access to equipment in Bay station. OLG was different because there was funding. OLG, by its nature, has

> significant technical resources. Organizationally, there was a lack of interest as well at the TTC in comparison with OLG. At OLG, there was interest from CEO through to technical staff. TTC had different priorities – I doubt that even with senior management approval [they would have] the expertise. [The TTC had] other major issues, had older generation of trains. It felt that TTC was more exploratory, unlike OLG.

Further, as quoted above, P7 adds that the project at the TTC may not have been, strictly speaking, a PbD project: "In other words, this project was looking at existing legacy system — it was not about designing a new system. It was retrofitting. Two options — put in a new system; or retrofit system to comply with PbD".

Whether or not it was a "true" PbD exercise, the research project failed to elevate the importance of privacy within the TTC. P6 describes the attitude towards privacy:

> Other than regulators and some privacy advocacy groups, most of [the TTC] doesn't [care especially] about privacy. So when you do the regulations, [privacy] becomes a checklist, and organizations who have generally [wanted] to implement a system which has a privacy impact to it, will pay a lip service to [privacy], and say yes, I designed it, I have a retention period that tries to address it … so I think that privacy becomes superficial.

2. The Role of the Internal Privacy Office

Interestingly, at the OLG, the internal access to information and privacy office had an insignificant role during the pilot project. P2 described it as "buried within the organization" and that its importance actually grew as a result of the success of the PbD project:

> I often sit back and say the whole privacy involvement started with this project. I mean people were aware, we had co-ordinators and stuff, but that was more [formal]. So now, right now at OLG if you think about it, in the project management life cycle, the privacy assessment, the central privacy assessment is right up front. It's very grained in the method.

P4 added: "this whole area of privacy by design and this policy was brand new at the time. Like privacy, when we started this program, privacy was, the whole privacy environment didn't have anywhere near the visibility it had today".

According to P5 as well, the importance of the privacy office grew after the success of the project:

> So we probably always had a privacy department at OLG, but I think it probably expanded or had a little more visibility because, I truly believe that was a very important piece. And they were using that as an example of also helping people understand what do you do, do a PIA, do a privacy impact assessment. Do it up front. Understand what you're doing, get it in at design time. Those terms, those little nuanced conversations about, even saying things like do it at design time. Those came from looking at [privacy] early.

3. Theme Summary

The findings related to the organizational theme, therefore, are that PbD initiatives, similar to any other initiative, need internal support in order to succeed. Internal support is required at all levels but, and significantly, even more so at the engineering level. Somewhat counterintuitively, the success or failure of the PbD initiative did not correlate with the existence of an active and visible privacy office within an organization, or even with the existence of a positive privacy culture. However, the success of a PbD initiative bolstered privacy after-the-fact throughout the organization.

C. The Regulator Theme

1. The Regulator's Role in Early Stages

It seems that in this case study, it was difficult, if not impossible, for participants to separate the role of the office of the IPC from the person that held that position for over eighteen years in Ontario. The paper discusses this duality further in the following section, but it was evident to participants that they had to deal not only with formal legalistic regulatory requirements but also with the personal convictions of the Commissioner. P1 put it in the following terms:

> I would say that Ann was really trying to take organizations into the next century … what made her very unique, is she was always looking for ways in which you could actually operationalize [privacy]. She wasn't just interested in reporting on it and investigating it, she wanted to know how to make it easier for people to do.

As P3 observed, the OLG knew that:

> to contemplate doing this without checking in with the regulator would have been death in Ontario. Because [the Commissioner was] very vocal, and always said to government departments "Come and talk to me. I will help you behind

> the scenes quietly".

P4 went further: "You know, the commissioner was not going to let us implement facial recognition without biometric encryption".

For P6, it seemed as well that PbD was more of a personal interest of the Commissioner than of the formal investigation:

> Prior to [the investigation], I don't ever recall the privacy by design aspect of that. So in the policy you're being driven to privacy, but not in a broad perspective, and then when they come out with a report in 2008, you're definitely getting the privacy by design aspects imposed in the recommendations and then in subsequent meetings with the privacy commissioner. You're no doubt getting the privacy by design speech [from the commissioner].

Going forward, P6 added that PbD could simply be viewed as the price that has to be paid in order to avoid greater regulatory scrutiny and obtain regulatory approval:

> When you look at 2007, [the TTC was] already into the investigation and you have the requirements imposed on [the TTC]. And therefore [the TTC doesn't] have a say, [it has to] meet the requirements. When [the TTC], prior to implementation, [goes] back to the regulators to sit with them, and work with them about what [the TTC does] with privacy by design, has much more attractiveness to me and why you get a far greater buy in. And the buy [in] isn't because they necessarily believe in it, the buy in is the price for [the TTC] to be able to do what it wants, and so that is the fundamental difference. So when you look at where [the TTC is] today, about front facing [cameras] or even audio, it is the TTC who has a far greater objective now, will be much happier to do something, will spend the dollars in order to appease everyone, and will implement and take a far greater active approach to privacy by design.

2. Regulatory Support for the Initiatives

In order to convince the OLG to consider PbD, the Commissioner not only raised concerns about the privacy implications of the new technology, but it appears that more importantly, the office offered support that exceeded traditional regulatory involvement. P3 described an initial meeting:

> We had this meeting in the boardroom, and [OLG CEO] laid this all out and she said I know [the Commissioner will] work with us to find a way to make this work. [And the Commissioner said] I have a solution but it has to be tested, a thing called biometric encryption.

And for P2, the regulatory, unconventional support was crucial to

accepting to take on a PbD approach:

> We had the perfect storm. You had an agency of the crown, who was interested in social responsibility. You have a privacy commissioner who had the privacy by design aspect, and had competent people in her organization. You had [the University of Toronto], and we were fortunate enough to get an Ontario company that actually did the facial recognition. With all that together, [PbD] worked.

P4 spoke about the support provided by the Commissioner and meeting the needs of multiple stakeholders:

> We had regular status meetings … we got like OLG, privacy commissioner, U of T, the vendor, and then we had the AGCO, and then we had the site management and gaming management … At this point in time, when you're running with multiple stakeholders, things get complicated. Too many people involved, [too] hard to do this work because you got too many stakeholders. In many cases, it can be really non-productive.

Despite the above lukewarm sentiments about the value of the regulator's support, P4 added:

> My sense is, and again since the privacy commissioner changed, right now we have almost no relationship with [the privacy commissioner]. We, the science guys here, have no relationship with the privacy office downtown at all.

P4's assessment fits the changes taken by the current IPC of Ontario, who has distanced himself and his office from the idea of PbD, for instance, by removing from the official website the numerous PbD resources that were created and promoted during the tenure of Cavoukian.

3. Primary vs Secondary Regulator

It appears that it was important for the success of PbD that the privacy regulator was "not" perceived as the primary regulator of the OLG (the TTC does not have a primary regulator). P4 provided an example: "as we started to move into the casino environment, to be able to do anything in the casino, you need the gaming regulator to be there … the regulator was there anytime you do anything in a casino".

And P5 stated more generally:

> There are big differences because the AGCO is the regulator of OLG. The privacy commissioner, yes, is a regulator as well, that's a part of the commissioner's office, but it's different, because we are like, that's a regulator of gambling, and we have massive amounts of gambling controls. It's done purely for protection and for control. The privacy commissioner is conceptual …

> Where at the AGCO, it's very direct, 'you will do this'.

4. Collaboration or Enforcement

Notably, following up on the previous theme, it seems that it was possible for the OLG to collaborate with the Privacy Commissioner as the secondary regulator and not be overly concerned about enforcement. In addition, Cavoukian's 3C approach played an important role in creating collaboration not only between the OLG and the Privacy Commissioner but between the TTC and the Commissioner as well. Noted P3: "Cavoukian always favoured the carrot to the stick, … from a privacy perspective. She would rather address things up front, rather than after a breach has happened".

Indeed, it seems that at least at the OLG, it was realized early on at the conceptual stage of the project that privacy issues would need to be addressed during the development of facial recognition for video surveillance technology (P1, P2 interviews). It was clear at the senior level that the privacy regulator would likely raise concerns with combining surveillance and biometric technologies that would involve collecting sensitive information on all casino patrons, not just the target (self-excluding) population (P1 interviews). Thus, there was an impetus to be proactive by reaching out to the Commissioner at the conceptual stage rather than after the design of the proposed system. At that point, it seemed that PbD would be an opportunity for collaboration with the regulator and that the PbD route would avoid the enforcement-style regulatory relationship. According to P4:

> OLG brought this forward to try and you know, talk to the privacy commissioner about using facial recognition … and I believe the privacy commissioner said no way … The privacy commissioner had published, or was getting ready to publish privacy by design … and was looking for use cases, or some experimental deployment to see if it would work. So [everyone] sort of put two and two together and said, OLG if you want to do this, we've got this privacy by design scenario, so would that work, would that be an opportunity.

At the TTC, the initial circumstances were different since there was already a complaint in front of the regulator about the use of CCTV within the TTC system. The complaint created a formal relationship of an investigation between the regulator and the TTC that did not

exist with the OLG. Prior to the complaint, it appears that an informal relationship did exist. States P6:

> The TTC had made public statements looking at cameras on the bus. So that adds a phone conversation and meetings with the Ontario Privacy Commissioner's office saying we want to help you, we want to see the policy, we will work with you on the policy.

The complaint, in other words, forced the regulator and regulated into an enforcement-style relationship where collaboration would have been preferable and, indeed, had been attempted. The focus was on the formal investigation led by the compliance, enforcement, complaints, and investigations department. Only later did the more collaborative research, policy, and special projects department become involved when looking at the potential privacy protective technology solution. Indeed, P6 did not recall PbD being front and centre in the initial conversations of the TTC with the Commissioner: "I did not recall that notion ever directly coming up, but it comes up indirectly. During the investigation, the answer is no". The TTC's focus was on the complaint and the investigation: "When you look at 2007, [the TTC was] already into the investigation and you have the requirements imposed on [the TTC]. And therefore [the TTC doesn't] have a say, [it has to] meet the requirements". However, at the later stage, with the involvement of the research, policy, and special projects department, the TTC was more receptive to PbD. According to P6: "When [the TTC], prior to implementation, [went] back to the regulators to sit with them, and work with them about what [the TTC will do] with privacy by design, [it] has much more attractiveness and why you get a far greater buy in".

5. The Overall Role of the Regulator

It was easier for the TTC and the OLG to approach the Privacy Commissioner given that the Commissioner at the time was Dr. Cavoukian who had (and continues to have) an unusually high public profile and a reputation for both forcefully advocating for privacy and strongly supporting organizations as they seek privacy-friendly solutions. P1 described the former Commissioner in the following terms: "It was Ann's openness to new solutions, and not immediately saying you

can't do that. And our openness to, you might have to do it differently, but we can get there". And P2 was impressed by the Commissioner's advocacy: "nobody would have thought that the information and privacy commissioner would be giving a talk at a gaming conference. And she did". Still P2 noted that the OLG approached the Commissioner with some trepidation: "there was a fear … because you're actually exposing the organization to the privacy commissioner … internally people were concerned".

P3 described the Commissioner's approach as follows:

> [The commissioner] developed the policy with 3 c's which was communication, co-operation, consultation. If you talked to [the commissioner] before the fact of whatever may have happened, then [they would] work with you behind the scenes, [not] trying to get any notoriety out of this. [The commissioner] wants solutions that work and wants to help you. You take all the credit.

Part of the Commissioner's advocacy was to change the internal thinking about privacy. P3 mentioned that the Commissioner had a presentation which said, "great privacy is a business issue, not a compliance issue, and a competitive advantage. Conflict with the regulator is a zero-sum approach".

P5 also felt that the Commissioner played a positive role:

> I think without Ann's passion for this, this never would have happened. I can guarantee you that. I would not have thought of even doing this. So, I would say that her passion for that, and the fact that she really you know, was adamant that we look at these things from a privacy lens very strongly, I think that that really helped. I think that the privacy commissioner's office really kept us on track. Kept the entire project, the program on track. OLG was a willing participant in it for sure, we all, we all wanted to make sure we did what was best for the public good, but I think that you needed that guidance for sure, it was key.

At the TTC, the overall relationship with the Privacy Commissioner had a different tone since the attempt to design privacy into the TTC's cameras was done alongside a formal investigation of a complaint about the TTC and its practices. While little was said by participants about the investigation itself, it seems that there were several barriers to adopting a PbD solution into TTC's video surveillance expansion, including the fact that the TTC did not come willingly to PbD adoption but that it was imposed through the investigation (P6 interview).

Still, the interaction with the regulator caused the TTC to formulate its need for surveillance cameras that would not have come about otherwise. States P6:

> The TTC said we want the regulator on board, we want to make sure what we're saying is perfect, and we want to work with [the regulator]. [The regulator] said, well you know, what we really want to know is have you looked at other less intrusive technologies, and what's the primary purpose, which is a problem to answer because every group has a different answer. So [the regulator] really just sent [the TTC] back, saying, this is what we want to see in the business case, show us that you've looked at all the other privacy [more protective options], and show me why they're not [possible], and then tell me how your system [will comply].

Finally, for P1, the role of the privacy regulator in contemporary society is different from the role of other regulators:

> Here's the thing though, where I think privacy is unique right now, there's such a proliferation of tools, to get into somebody's information. I think by virtue of the environment, there is a stronger need for the regulator to have much more proactive foresight on where to get ahead of this, and also to be working collaboratively with insight on how to design. I don't think any legislative regulator in the area of privacy and information in what is now, basically, a data-driven analytics age, can be resting on their historical way.

To that P3 added:

> [The commissioner's role is] not a traditional role. Perhaps because [Cavoukian was] not a lawyer, it was easy for her to look at it as not a lawyer. [Cavoukian] loved the design aspect, let's design things in a way that can avoid the need to engage the regulators wrath, which is usually what you're getting at the end.

6. Theme Summary

The sum of the findings related to the regulator theme is that the personal role that Ann Cavoukian played in the implementation of PbD is inseparable from the formal regulatory role that her office played. It is clear that regulatory support early-on was crucial for the success of PbD and also that the formal regulatory relationship, in the form of an investigation, was, in fact, counter-productive and did not lead to the success of PbD. Broadly speaking, it seems that a collaborative regulatory model is preferable to a model which focuses on the enforcement of the relevant privacy law and that an informal relationship, such as the one that is created when the Privacy Commissioner is perceived not to be the

main regulator, is preferable to a more formal one for such initiatives to succeed.

V. Conclusions

Three conclusions can be drawn from the findings of this research project with respect to engineering privacy, privacy as an organizational function, and finally with respect to regulating PbD.

A. Privacy as an Engineering Problem

Privacy continues to be an engineering problem. Ten years ago, in both initiatives, the first and foremost challenge was to engineer a technological solution that would reflect in a meaningful way the principles of PbD. In both initiatives, engineers at all levels of the project noted their inability to use the principles of PbD in a way that would help them in their work.

At the TTC, the initiative did not proceed beyond some preliminary testing. The findings show that the TTC did not find the biometric encryption technology useful. This was a straightforward conclusion that, in fact, had little to do with PbD. Simply put, the technology did not work in the manner that the TTC had hoped for, or in a manner that at least would garner support for the continuation of the initiative. During the limited pilot, PbD and its principles were of limited use to the researchers and engineers as they attempted to incorporate the privacy enhancing technology into the TTC's systems. PbD could not offer, therefore, professional guidance, the equivalent of an engineering manual, to the researchers working on the initiative and could not point them in the direction of a successful solution. PbD was of little practical use and due to the overwhelming lack of organizational support for the initiative within the TTC, could not even play a motivational, inspirational, or ideological role.

At the OLG, with all of the senior leadership support and with all of the regulatory support, the initiative came close to failure because of the difficulty of engineering PbD. In a sense, as revealed in the findings, the original initiative did fail, and it became apparent that it was necessary to reconfigure the project to allow for some form of integration of biometric encryption into the facial recognition systems that the OLG was preparing

to deploy. From the initial hope (and perhaps, to this day, widespread public misperception) that PbD would protect the information of all visitors to the OLG gambling sites by encrypting their images,[55] and in so doing would mitigate the risks of such information being shared with others for a variety of secondary, unapproved purposes, the OLG initiative changed to deploy biometric encryption in order to enhance the security of its self-excluded patron database. The images of such patrons are used, in other words, as an encryption key that unlocks the database upon the entry of a self-excluded patron into an OLG gambling site.

The OLG initiative can hardly be said, therefore, to diminish surveillance or the use of CCTV or the use of facial recognition technology. However, the OLG initiative does demonstrate the successful incorporation of privacy enhancing technology into its image processing and databases. The question remains whether the initiative was an example of the successful application of PbD principles to a technological problem and whether we can conclude that PbD principles provided guidance to the OLG's engineers as they attempted to incorporate biometric encryption into their systems. The findings unfortunately indicate that we cannot and that the PbD principles were mapped onto the work done by engineers after the fact and with some difficulty. At best, PbD inspired all those working on the initiative to indeed find a way to design privacy protection into it. The importance of PbD as a motivating factor and driving force is, therefore, an important conclusion, yet at the same time it underscores the important realization that the principles of PbD offer little practical guidance to engineers.

---

55. One of the very first paragraphs of the report on the OLG initiative, IPCO, "Privacy-Protective Facial Recognition", *supra* note 50 states "the increased use of facial recognition technology raises a number of privacy and security concerns. Given their mutual interest in respecting the privacy of all casino patrons, the IPC and OLG agreed that the application of an emerging Privacy-Enhancing Technology — Biometric Encryption (BE) — to a facial recognition system at an OLG casino would be an ideal 'win-win' project" at 1. See also IPCO, "Privacy-Protective Facial Recognition", *supra* note 50 at 14.

B. Privacy, Organizational Change, and Leadership

Against the backdrop of difficulty in implementing PbD in a technical, engineering sense, there is a growing sense that the value of PbD lies more in its ability to bring about organizational change and serve as an effective leadership tool. The findings allow for a discussion of the importance of regulatory leadership as well, which is discussed in the following section.

The two initiatives present radically different, almost diametrically opposed, organizational approaches.[56] At the TTC, it is clear that there was little appetite for organizational change. Leadership viewed the PbD initiative as a regulatory imposition that was foisted upon the organization as a result of an external complaint. Indeed, it seems that the organization was at a loss understanding why a formal investigation against it was launched when, from an organizational perspective, existing systems and policies were reviewed and vetted by the IPC. From the outset, therefore, the TTC appeared to be in organizational opposition to any attempt to enhance or design privacy into its systems, possibly because that would be tantamount to admitting that the systems needed to be enhanced and were, therefore, lacking in some way and that the complaint against it would somehow, as a result, be perceived as justified.

Adding to the organizational reticence was the formal complaint process and the formal relationship that it created between the TTC and the IPC. As an organization, the TTC appeared content to remain within the confines of the complaint process and not venture beyond. Since the exploration of privacy enhancing technology was formally one of the recommendations of the IPC's investigatory report, the TTC dealt with it formally, and perhaps with minimal effort, in order to ensure it was in compliance with the report but not really out of a compelling interest in privacy. PbD was perceived not as a motivating ideology but as an imposition.

---

56. This point is strengthened by the recognition that both initiatives appeared to benefit from similar organizational resources. The TTC, for instance, provided access to its subway stations and other facilities in order to provide researchers the ability to evaluate their PbD technology for the duration of the initiative.

At the TTC, there was no push at the time to introduce new, potentially invasive, potentially surveilling, technology. The organization had its priorities set out in terms of improving service levels, increasing and maintaining ridership levels, improving customer experiences, maintaining costs, etc. It was focused on its core mandate of providing transit services, and as a result, leadership viewed the investigation, report, and pilot project as unwelcome distractions. In this organizational environment, there was little room for PbD to take hold, let alone serve as a useful tool for leadership.

In contrast, the approach of the OLG to PbD was strategic and calculated in order to ensure regulatory support for the organization's initiative to modernize its self-exclusion program. Leadership of the OLG, at its most senior levels, was committed to support the integration of privacy with the facial recognition technology it was interested in. The findings indicate that the OLG leadership recognized the value of privacy not only strategically, in its dealing with the IPC, but also as a genuine value of public policy. As such, the protection of privacy fitted other values that the OLG aspired to associate with, such as organizational social responsibility in the context of responsible gaming.

The organizational adoption of PbD was easier at the OLG for two additional reasons. First, the OLG was not caught up in an investigation and was not the subject of a complaint to the IPC. The OLG was, therefore, not constrained by a formal relationship or concerned with the implications any of its actions may have with respect to an ongoing investigation. Second, the IPC was not the primary regulator of the OLG, allowing for a free and more informal relationship between the two entities. It is clear from the findings that the OLG is very careful in its relationship with its primary regulator, the AGCO, and that the regulatory guidance of the AGCO is quite detailed at times. It is telling that the OLG perceived the IPC and PbD as the opposite, and this further supports the conclusion that the power of PbD is not to be found in detailed technical guidance but rather in its ability to increase awareness and motivate organizations to think about privacy from the outset.

Once the leadership of the OLG endorsed privacy and endorsed PbD as the approach that should be taken with respect to its facial

recognition initiative, it was able to instill within its engineers working on the project the necessity of taking privacy into consideration and of collaborating openly with the IPC on a privacy enhancing solution. The IPC was perceived not so much as a dreaded regulator but rather as a subject-matter expert brought in to assist on the incorporation of privacy and on the understanding of PbD. This open relationship enabled close collaboration (of which adherents of a more formal regulatory role may be critical — see the following section) and ultimately allowed for the OLG to change the manner in which biometric encryption was integrated into its systems with the approval of the IPC.

The internal organizational result, as evidenced by the findings, has been an increase in the role and significance of privacy throughout the OLG from a more formal, limited, compliance role to a more pervasive, cultural, strategic role. Participants became more familiar and comfortable with PbD and its principles (such as purpose specification), the privacy office has increased in its resources and organizational importance, and privacy impact assessments are no longer a novelty. All of this occurred, notwithstanding the difficulties that the OLG's engineers had with the actual implementation of PbD's principles into their processes. This result strengthens the overall conclusion that the importance of PbD can be found in its ability to effect change, to inspire and to motivate, rather than in its ability to provide detailed guidance on how privacy is to be designed into a specific, given project. Of course, such conclusions have implications with respect to the ideal regulatory role in enforcing PbD once it becomes legally required.

C. PbD as a Regulatory Tool

As noted in the second section of this paper, Article 25 of the *GDPR* (that section of the new EU legislation where PbD is introduced into law) states that organizations will have to "implement appropriate technical and organisational measures … which are designed to implement data-protection principles … , in an effective manner and to integrate the necessary safeguards into [data] processing".[57] The Article also states that

57. *GDPR*, *supra* note 1, art 25(1).

in so doing, organizations must take several factors into account:

> the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[58]

Finally, the Article states that organizations will be able to demonstrate compliance through certification. As envisioned in the *GDPR*, certification will be a voluntary process undertaken by organizations, and certificates and seals will be issued by certifying bodies that are, in turn, accredited by the relevant data protection authorities.[59]

Several important points emerge from the language used in the *GDPR* with respect to PbD. First, PbD is not understood exclusively as a technical or engineering tool. It is just as equally an organizational tool that can be used to bring about organizational measures and changes that will better protect privacy. The findings discussed above, and in particular the immediate conclusion above with respect to the ability of PbD to bring about organizational change, support Article 25 to that extent.

Second, Article 25 recognizes that PbD is an exercise that will vary greatly from one set of circumstances to the next and that in order to succeed as a regulatory instrument, PbD will have to take into account the factors listed in Article 25. This language indicates that a heavy-handed, one-size-fits-all regulatory approach is not to be expected in the EU with respect to PbD and that organizations will be given considerable flexibility. Unfettered flexibility does raise concerns, of course, as to whether PbD will end up as a watered-down idea that will not bring about meaningful regulatory change. Yet, at the same time, this case study does indicate that flexibility, and in particular regulatory flexibility with respect to the implementation of PbD, is necessary if the idea is at all to succeed.

This flexibility is discussed further immediately below, but even prior to that discussion, it is worth noting how different the regulatory paths of the two initiatives were, despite apparent similarities. The OLG and the TTC both explored very similar intrusive technology, and both were

58. *Ibid*.
59. *Ibid*, art 42–43.

subject to the same legal framework surrounding personal information in Ontario. However, these similarities only serve to emphasize the different outcomes of each initiative. As discussed above, the initiatives ended differently largely due to the degree of internal organizational support each initiative enjoyed but (and perhaps more importantly for the present discussion and for the more general discussion attempting to determine how PbD will fare when it is mandated by law) also due to the role of the regulator in each initiative.

Throughout the TTC initiative, the regulator was constrained by the formal investigation and could not collaborate with the TTC to push for the success of PbD. With the OLG, however, due to the combination of not being the main regulator of the OLG as well as not formally investigating the OLG, the IPC was able to actively collaborate and demonstrate considerable flexibility. From a PbD initiative, which was presented to the public and perceived as an initiative in which privacy would be designed into surveillance cameras using innovative bio-encryption technology so that all individuals walking into an OLG gambling facility would have their privacy protected (through the encryption of their image), the project changed in scope to provide, in the end, for the protection of the personal information of self-excluded patrons in the OLG database by encrypting it with their image. While a noteworthy and laudable achievement, the final outcome of the OLG initiative is a far cry from its original formulation. It is clear from the findings that it would not have developed in such a manner were it not for the approval of the IPC and (then) Commissioner Cavoukian specifically.

Information gathered during the interviews conducted for this project was not sufficient to determine conclusively why such a change took place. Was it so that the OLG could simply proceed uninterrupted in the modernization of its self-exclusion program? Was it so that the OLG and the IPC could showcase a model of regulated-regulator interaction? Was it so that the IPC could tout PbD as a workable and not only aspirational idea? Was it to demonstrate the benefits of bio-encryption as a specific form of privacy enhancing technology? In all likelihood, the answer is a mix of all of the above. Does that indicate that Cavoukian cared more

about demonstrating the success of bio-encryption and of PbD than she did about the protection of everyone that would walk into a casino? Although Cavoukian has been forcefully criticized for her 3C approach and her pragmatism in the past,[60] such a conclusion seems unduly harsh.

A more positive evaluation of Cavoukian and the IPC's role would take into account her creation of a research, policy, and special projects department, the substantial support her office gave to the two initiatives through this special department, and her regulatory flexibility, all as much-desired regulatory traits. The findings can be further used to argue the point that neither initiative would have enjoyed the same level of support under another commissioner. Indeed, no other regulatory office in Canada has supported PbD initiatives in a similar manner, and the research, policy, and special projects department no longer exists at the IPC.

Regulatory determination, even rigidity, is no doubt quite often necessary and required, and the IPC, including under Cavoukian, certainly has shown its ability to enforce the law and exercise its order-making powers under Ontario's provincial legislation. The question of this case study is, however, whether PbD will be better achieved through a rigid or flexible approach. In the United States, for example, the introduction of PbD led scholars to call on the Federal Trade Commission ("FTC") to combine some regulatory firmness ("enforcement threats") with the cultivation of "entrepreneurial privacy [advocacy]" and in so doing to "[avoid] both the shortcomings of static, top-down, command-and-control regulatory approaches and the ways in which reliance on bottom-up self-regulation alone can subvert public goals by private interests".[61] It is certainly understandable why the IPC and Cavoukian would want to demonstrate flexibility with respect to PbD at a time that it was not explicitly part of the governing law but rather an approach that the IPC

60. Ian Kerr, "Dreamin Man: The Role of Idealism and Pragmatisms in Privacy Advocacy" *Ian Kerr* (23 July 2008), online: Ian Kerr <www.iankerr.ca/blog/2016/6/21/dreamin-man-the-role-of-idealism-and-pragmatisms-in-privacy-advocacy>.

61. Kenneth Bamberger & Deirdre Mulligan, "Privacy on the Books and on the Ground" (2011) 63:2 Stanford Law Review 247 at 313.

encouraged organizations to take with respect to compliance.

More generally (and to the extent that the case study can be generalized), it appears that a rigid approach to the implementation of PbD would be counter-productive given the ambiguity surrounding many of the operational details that have been developed, or have been attempted to develop, with respect to PbD over the years. PbD has always been most impactful as a guiding principle, emphasizing the importance of privacy and elevating privacy to the level of other organizational goals by stressing that it should be included in every organizational initiative related to personal information. The TTC and the OLG initiatives show us (in addition to academic literature on this point) that mapping PbD onto engineering, solution, and design algorithms is incredibly difficult. Some flexibility is, therefore, almost essential given the present state of PbD.

It may be that, somewhat intuitively, Cavoukian adopted a flexible regulatory approach that both fits PbD and appears to be advocated for increasingly by scholars studying the data protection authority model and its efficacy over the years. Researchers that examine information systems have argued that PbD will only succeed if it is applied as part of a contextual approach rather than by attempting to quantify privacy.[62] Scholars have called, for example (and specifically with respect to PbD), for an innovative regulatory framework that will allow, if not encourage, experimentation with new technological and engineering solutions and that will facilitate agreements between organizations and regulators that are the product of discussion and negotiation.[63] On both counts, that is very similar to the conduct of the IPC in this case study.

D. The Future of PbD

How will PbD flourish now that it is about to become law in one of the largest jurisdictions in the world? This case study instructs us that it is probably not possible to develop a uniform mapping of PbD principles onto engineering and solution design. The two initiatives demonstrate just

62. Davies & Langheinrich, "Privacy by Design", *supra* note 53.
63. Rubinstein, "Regulating Privacy by Design", *supra* note 18.

how difficult it was to achieve even partial success in the implementation of PbD under what could be seen as almost ideal circumstances, of an encouraging and supportive regulator and enthusiastic (at least in the case of the OLG) organizational response. The difficulties, if not outright failure, of coherently engineering PbD point not only at the weakness of the concept but at its strength. PbD is best realized as a rallying call for privacy, as a change and leadership tool that can be used internally in an organization but also externally by the regulator.

How should European and other regulators approach PbD therefore? It seems from the case study that a mix of rigidity and flexibility is required. Rigidity is required with respect to insistence on the principle itself — that privacy must be and become a priority, that initiatives are not to proceed without privacy in mind, that privacy must be the default (in the language of Article 25). All of these should not be subject to compromise and negotiation between the regulator and regulated. Yet at the same time, the case study instructs us that regulatory flexibility with respect to the implementation of PbD in specific initiatives is absolutely required. PbD will fail if regulators develop and insist upon a uniform approach to its application.

It is likely that certification will play a significant role in the creation of this regulatory flexibility, not because of the substantive standards of certification, which could be quite detailed and quantitative, but simply by virtue of introducing intermediaries in between the regulator and the regulated. In a sense, regulatory rigidity as it relates to the details of what it means, organizationally to design privacy, will be outsourced to the certifying bodies, allowing the supervising (data protection) authorities leeway in the determination of whether specific organizations and initiatives are in compliance with Article 25. Interestingly, Cavoukian, through her PbD Centre of Excellence at Ryerson University, and in partnership with the accounting firm Deloitte, is one of the first bodies

to offer such certification.[64]

Certification, and indeed the idea of PbD itself, can also be seen as carrots offered to organizations by law instead of a heavy regulatory stick. The regulator, according to this understanding, will step back and not micro-manage the protection of privacy by organizations, but in exchange, organizations must respond by changing internally and turning privacy into one of their leading values. And that, learning from the case study, is what appears to have happened at the OLG. The IPC let the OLG facial recognition proceed at a cost to the privacy of the many visitors to the OLG's gambling sites but received the benefit of a changed organization that now has greater awareness to privacy and that willingly accepts the design of privacy into any future initiative.

The risks of such a regulatory "bargain" are clear yet may be unavoidable due to the limitations of PbD. Is the Ontario case study a red flag, a signal cautioning against determined regulatory flexibility at the expense of privacy protection? Or is it a demonstration, well ahead of its time, of a bold, new, and unconventional regulatory approach? Time will tell if this regulatory flexibility, this compromise of individual protection in consideration for organizational awareness and change, is the approach that regulators should take and whether designing privacy in such a manner will lead to the desired outcome that the *GDPR*, and similar regulatory frameworks, are intended to deliver: Privacy.

64. For some instructive details as to how Cavoukian certifies organizations, see Sylvia Kingsmill, "Privacy by Design Assessment and Certification" *Deloitte* (October 2017), online: Deloitte <www.ryerson.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology.pdf>.

Appendix: Interview Questions

1. What is your professional background?

2. What is your current role, and what was your role in connection with the policy of "privacy by design" that we will discuss today?

3. Please tell me about this policy:

    a. Who initiated the policy?

    b. What was the motivation for the new policy?

    c. What inspired this policy? (*e.g.* Ontario's Privacy Commissioner; the "Jerusalem declaration" of the Privacy Commissioners from 2010). What were the considerations underlying the policy and what is its purpose?

    d. What was the decision-making process concerning the implementation of the policy? (who decided, who was consulted, what preliminary steps were taken, etc.)

    e. What interaction did you have with the regulators? Was it direct (*e.g.* meetings, correspondence) or indirect? (*e.g.* reading reports)

    f. Were the implications of the policy examined? How?

4. What was the underlying concept of privacy that this policy addressed? How was the policy intended to meet the privacy needs?

5. What was the concept that founded the regulation of technological activities by legal means? Did the ability to implement the policy depend on the technology you were addressing?

6. What was the role of engineers (*e.g.* computer), and were they part of the public or private sector in the implementation of the policy? How did engineers influence the outcome?

7. What role did having or being dictated a policy have in the internal

organizational discussion about privacy?

8. How is the policy implemented in practice? Are there difficulties in its implementation? What are they? Is the policy achieving its privacy and more general objectives?

Abandoning The "High Offensiveness" Privacy Test

N.A. Moreham*

This article argues that the New Zealand torts of giving publicity to private information and intruding upon solitude and seclusion would better reflect the true nature of the privacy interest if the requirement that any alleged privacy interference be "highly offensive to an objective reasonable person" were abandoned. Courts should, instead, determine what is prima facie private by reference to the plaintiff's "reasonable expectation of privacy" in respect of the information or activity in question. There are three main reasons for this: first, the high offensiveness test operates in a manner which is both uncertain and unpredictable; second, New Zealand courts applying the high offensiveness test have taken too narrow a view of the nature of privacy harms; and third, the test is unnecessary.

* Reader in Law, Victoria University of Wellington. I would like to thank Marcin Betkier, Victoria University of Wellington, for his careful copy-editing assistance. I take full responsibility for all content.

I. Introduction
II. The High Offensiveness Test in New Zealand Law
III. Doubts About the High Offensiveness Test
IV. Why the High Offensiveness Test Should Be Abandoned
A. Lack of Principle in the Application of the High Offensiveness Test
B. Taking Too Narrow a View of Privacy Harms
C. The High Offensiveness Test is Unnecessary
V. Conclusion

I. Introduction

The common law protection of privacy in the Anglo-Commonwealth has blossomed in the last fifteen years. New Zealand and Ontario have recognised torts both of giving publicity to private facts and of intrusion into solitude and seclusion and in England and Wales, the tort of misuse of private information has emerged from within the breach of confidence. Two main approaches to ascertaining what is private have emerged from these developments. On the one hand, courts applying the English misuse of private information tort focus on the plaintiff's reasonable expectations of privacy (which in turn determine whether the plaintiff's right to respect for private life under Article 8 of the *European Convention on Human Rights*[1] is "engaged") and on any competing public interest in the material. On the other hand, there is the more complex Ontarian and New Zealand approach of asking not just whether the information or activity is private — which is usually determined by reference to reasonable expectations of privacy — but also whether the intrusion or publicity in question would be highly offensive to an objective reasonable person.

This article will argue that the first of these approaches — determining what is private by reference to reasonable expectations of privacy — is better. It does so by highlighting the many shortcomings of the operation

1. *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 art 8 (entered into force 3 September 1953).

of the high offensiveness requirement in New Zealand law and by contrasting it with the simpler English approach. The article begins by explaining both the rationales for and doubts about the New Zealand high offensive test. Three reasons for abandoning the requirement are then given. First, the relative lack of principle governing the application of the high offensiveness test makes it uncertain and unpredictable. Second, where principles have been developed, courts have taken too narrow a view of the nature of privacy harms (which in turn obfuscates the dignity and autonomy interests at heart of the privacy action). Third, the article shows that the high offensiveness test is unnecessary.

II. The High Offensiveness Test in New Zealand Law

The New Zealand privacy torts have at their heart ideas of retreat and inaccessibility. They protect people's ability to remove themselves from the world and to keep certain information to themselves; in other words, to carve out a realm in which they can choose, on their own terms, the extent to which they are accessed by others. As Justice McGrath said (citing this author) in the Supreme Court case of *Brooker v Police*,[2] privacy is therefore an aspect of human autonomy and dignity which protects against unwanted access to one's physical self and private information.[3] Justice Tipping agrees. In the leading New Zealand Court of Appeal decision, *Hosking v Runting*,[4] he says:

> Privacy is potentially a very wide concept; but, for present purposes, it can be described as the right to have people leave you alone if you do not want some aspect of your private life to become public property. Some people seek the limelight; others value being able to shelter from the often intrusive and debilitating stresses of public scrutiny. … It is of the essence of the dignity

2. [2007] NZSC 30.
3. *Ibid* at para 123, citing Lord Hoffmann in *Campbell v MGN Ltd*, [2004] UKHL 22 at para 50 [*Campbell HL*] and citing N A Moreham at para 253 in "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121:4 Law Quarterly Review 628 at 640–41. See also *ibid* (Thomas J's description of the home as a "sanctuary", a place "to retreat or repair to" at para 257).
4. [2004] NZCA 34 [*Hosking*].

> and personal autonomy and well-being of all human beings that some aspects of their lives should be able to remain private if they so wish. Even people whose work, or the public nature of whose activities make them a form of public property, must be able to protect some aspects of their lives from public scrutiny.[5]

New Zealand appellate courts first recognised tortious protection of these privacy interests in 2004 in the *Hosking* case just mentioned.[6] In that case, a television presenter and his former wife (acting on behalf of their 18 month old children) sought to prevent a women's magazine from publishing photographs of the children being wheeled down a busy Auckland shopping street in a push chair by their mother. The plaintiffs claimed that the photographs breached the children's privacy and, given the celebrity of the first plaintiff, potentially jeopardised their safety. All five judges agreed that there was no breach of privacy in the circumstances (primarily because the photographs were of an innocuous event which took place in public), but three of the five nonetheless held that there was a tort of giving publicity to private facts in New Zealand.

In the more widely cited of the two majority judgments, Justices Gault and Blanchard held that the publicity tort has two main requirements. The plaintiff, first, has to establish the existence of facts in respect of which

---

5. *Ibid* at paras 238–39. These views are echoed elsewhere in the common law world. For example, in an oft-cited passage from the leading English privacy tort case of *Campbell HL*, *supra* note 3 Lord Hoffmann said that "the protection of human autonomy and dignity — the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people" at para 51. Blatz CJ similarly says in the Supreme Court of Minnesota in *Lake v Wal-mart Stores Inc* (1998), 582 NW (2d) 231 (Minn Sup Ct (US)) that: "The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close" at 235.

6. *Hosking*, *supra* note 4. The tort had previously been recognised in a handful of first instance decisions including *Tucker v News Media Ownership Ltd*, [1986] 2 NZLR 716 (HC) [*Tucker*]; *Bradley v Wingnut Films Ltd*, [1993] 1 NZLR 415 (HC) [*Bradley*]; *P v D*, [2000] 2 NZLR 591 (HC) [*P v D*].

there is a reasonable expectation of privacy and second, that publicity was given to those private facts that would be considered highly offensive to an objective reasonable person.[7] Gault and Blanchard JJ made it clear that the first requirement — that the plaintiff had a reasonable expectation of privacy — is designed to determine whether the information in question was private. Under the heading "Private Facts", they explained (citing Chief Justice Gleeson in the Australian High Court case of *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*)[8] that there is no bright line between what is public and private but that:

> Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved.[9]

The third member of the majority, Tipping J, agreed that whether there is a reasonable expectation of privacy depends on social mores, stating that the word "reasonableness" plainly imports into the privacy tort an enquiry into "contemporary societal values" in respect of the matter at hand.[10] Gault and Blanchard JJ took account of a range of factors in deciding that the children had no reasonable expectation of privacy in that case including the plaintiffs' location, the nature of the activity depicted, public accessibility of the "facts" which the photograph conveyed (which they said, were the existence of the twins, their age, and the fact that the parents were separated), and the plaintiffs' particular attributes including the fact that they were children and that they had a celebrity parent.[11]

Importantly for the purposes of this article, according to Gault and Blanchard JJ, but not Tipping J, a plaintiff seeking to establish an actionable breach of privacy also has to satisfy a second test. He or she

---

7. *Hosking*, *supra* note 4 at para 117.
8. [2001] HCA 63 [*Lenah*].
9. *Hosking*, *supra* note 4 at para 119 citing *ibid* at para 42.
10. *Hosking*, *supra* note 4 at para 250.
11. *Ibid* at paras 120–24, per Gault and Blanchard JJ and at para 260, Tipping J also took account of the plaintiffs' location and his assessment of likely societal attitudes to the image.

has to show that publicity was given to the facts in question which would be highly offensive to an objective reasonable person.[12] The inspiration for this came particularly from three sources:[13] the United States tort of giving publicity to private life (as articulated in the *Restatement of the Law of Torts (Second)*);[14] Gleeson CJ's statement in *Lenah* that "[t]he requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private";[15] and the English Court of Appeal's application of the high offensiveness test in *Campbell v MGN Ltd*[16] (which, as discussed below, was subsequently overruled by the House of Lords).

Gault and Blanchard JJ make it clear that the point of the high offensiveness test is to ensure that trivial claims are excluded from the reach of the publicity tort. They said that although a rights-based action like breach of privacy would usually be actionable irrespective of "the seriousness of the breach", "it is quite unrealistic to contemplate legal liability for all publications of private information".[17] It would be "absurd" they said "to consider actionable merely informing a neighbour that one's spouse has a cold":[18] rather "[b]y living in communities individuals necessarily give up seclusion and expectations of complete privacy".[19] They go on to explain that the action should only be concerned with

12. *Ibid* at para 117.
13. *Ibid* at para 126.
14. William L Prosser, John W Wade & Frank J Trelease, *Restatement (Second) of Torts* (Philadelphia: The American Law Institute, 1977) (which says that the publicity tort requires a plaintiff to show that "the matter publicised is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public" at § 652D) [*Restatement of Torts*]. Early High Court decisions recognising the right to privacy in New Zealand were also heavily influenced by US law; see *e.g. P v D*, *supra* note 6 at paras 33–34 and *Bradley*, *supra* note 6 at 423 *et seq*.
15. *Lenah*, *supra* note 8 at para 42.
16. [2002] EWCA Civ 1373 [*Campbell CA*].
17. *Hosking*, *supra* note 4 at para 125.
18. *Ibid*.
19. *Ibid*.

"*widespread* publicity of very personal and private matters"[20] and that:

> publicity, even extensive publicity, of matters which although private, are not really sensitive should not give rise to legal liability. The concern is with publicity that is truly humiliating and distressful or otherwise harmful to the individual concerned. The right of action, therefore, should be only in respect of publicity determined objectively, by reference to its extent and nature, to be offensive by causing real hurt or harm.[21]

Finally, they stressed that the high offensiveness test relates to "the publicity" and is not part of the test of whether the information is private.[22]

Although there has always been doubt about the desirability of this separate highly offensive publicity requirement, Gault and Blanchard JJ's approach has been consistently applied in subsequent first instance decisions.[23] Importantly, this includes the 2012 case of *C v Holland*[24] in which New Zealand's second privacy tort — the tort of intrusion into seclusion — was first recognised.[25] In that case, a woman successfully sued her flatmate for damages after he videoed her through a hole in the ceiling while she was having a shower. Proceedings were brought to establish the preliminary issue of "whether invasion of privacy of this type, without publicity or the prospect of publicity, is an actionable tort in New Zealand".[26] Justice Whata held that it was, regarding the tort of intrusion into seclusion as "entirely compatible with, and a logical adjunct to, the *Hosking* tort of wrongful publication of private facts".[27] Whata J

---

20. *Ibid* [emphasis added].
21. *Ibid* at para 126.
22. *Ibid* at para 127.
23. See *e.g. Andrews v Television New Zealand Ltd*, [2009] 1 NZLR 220 (HC) [*Andrews*]; *Faesenkloet v Jenkin*, [2014] NZHC 1637 [*Faesenkloet*]; *Brown v Attorney-General (Invasion of Privacy)*, [2006] NZAR 552 (DC) [*Brown*].
24. [2012] NZHC 2155 [*Holland*].
25. *Ibid*. The existence of the seclusion tort in New Zealand has been implicitly accepted in a handful of cases since, including in the Court of Appeal in *Graham v R*, [2015] NZCA 568 at para 22 *et seq*.
26. *Holland*, *supra* note 24 at para 1. (The case settled before the substantive hearing took place.)
27. *Ibid* at para 75.

held that the New Zealand intrusion tort has four key requirements:

(a) An intentional and unauthorised intrusion;

(b) Into seclusion (namely intimate personal activity, space or affairs);

(c) Involving infringement of a reasonable expectation of privacy; and

(d) That is highly offensive to a reasonable person.[28]

A legitimate public concern in the "information" may provide a defence.[29]

Whata J's formulation of the intrusion into seclusion tort was once again heavily influenced by North American jurisprudence, this time by both the US and new Ontarian intrusion torts.[30] In Whata J's view, it was important to develop the requirements of the action consistently with those actions so that the New Zealand torts could benefit from the guidance which North American authority provides. He also stressed the need to ensure that the "content" of the intrusion tort is consistent with domestic privacy law and principles.[31] Whata J therefore preferred his four-part approach to the one-step English reasonable expectation of privacy test, holding that the English approach "is not sufficiently prescriptive"[32] and that the conflict between the right to seclusion and other rights and freedoms is "very significant" and demands "a clear

28. *Ibid* at para 94.

29. *Ibid* at para 96.

30. *Ibid* at paras 11–17, 94. According to *Restatement of Torts*, *supra* note 14, "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person" at § 652B. The question of whether there is an intrusion upon seclusion is determined by reference to the plaintiff's reasonable expectation privacy in respect of the place or matters intruded upon (see *Shulman v Group W Productions, Inc*, 18 Cal (4th) 200 (Cal Sup Ct (US) 1998)) [*Shulman*]. According to *Jones v Tsige*, 2012 ONCA 32 [*Jones*], a plaintiff seeking to establish the Ontarian tort of seclusion must show "(1) an unauthorised intrusion; (2) that the intrusion was highly offensive to the reasonable person; (3) the matter intruded upon was private; and (4) the intrusion caused anguish and suffering" at para 56.

31. *Holland*, *supra* note 24 at para 94.

32. *Ibid* at para 97.

boundary for judicial intervention".[33] In his view, the high offensiveness test sets a "workable barrier to the unduly sensitive litigant".[34]

III. Doubts About The High Offensiveness Test

In spite of its consistent application in first instance decisions, the desirability of a separate high offensiveness test in New Zealand law has always been a matter of contention. Significantly, Tipping J did not see any need for it in *Hosking*. Although he agreed with Gault and Blanchard JJ that "relatively trivial invasions of privacy should not be actionable"[35] and that "it will always be necessary for the degree of offence and harm to be substantial",[36] in his view the separate high offensiveness requirement set the bar for recovery too high and was unnecessary. This was because the reasonable expectation of privacy test could be relied on to exclude unmeritorious claims:

> I would myself prefer that the question of offensiveness be controlled within the need for there to be a reasonable expectation of privacy. In most cases that expectation is unlikely to arise unless publication would cause a high degree of offence and thus of harm to a reasonable person. But I can envisage circumstances where it may be unduly restrictive to require offence and harm at that high level …[37]

He continued that regardless of whether it forms part of the reasonable expectation of privacy test or operates as a separate test, any "qualifier" used to determine whether something is private should be a "substantial level of offence" rather than a high level of offence. The former, he said, was "more flexible, while at the same time capturing the essence of the matter".[38]

Other judges — including members of the New Zealand Supreme Court — have also questioned the status of Gault and Blanchard JJ's test, particularly the desirability of the highly offensive publicity requirement.

---

33. *Ibid*.
34. *Ibid*.
35. *Hosking*, *supra* note 4 at para 255.
36. *Ibid* at para 256.
37. *Ibid*.
38. *Ibid*.

In the Supreme Court decision of *Rogers v Television New Zealand*,[39] two of their Honours applied Gault and Blanchard JJ's test but expressly declined to approve it.[40] Chief Justice Elias, with whom Justice Anderson concurred, also said that the Court should "reserve its position on the view … that the tort of privacy requires not only a reasonable expectation of privacy but also that publicity would be 'highly offensive'", noting that the test had been "doubted" by members of the House of Lords in the leading English decision of *Campbell*.[41] Similar reservations can be gleaned from the judgment of President Young in the Court of Appeal decision in *Rogers*. Echoing Tipping J in *Hosking*, he said:

> These two elements are interconnected. In most cases it will be the defeating of a reasonable expectation of privacy which makes publication objectionable, and likewise if publicity could fairly be seen as objectionable that might well suggest that there was a reasonable expectation of privacy in relation to the information in question. For present purposes, however, I propose to focus on the first of these two requirements.[42]

These observations also reflect concerns raised by numerous commentators about the impact of the high offensiveness test on the New Zealand privacy

39. [2007] NZSC 91.
40. *Ibid* at para 99, per McGrath J at para 144, per Anderson J at para 46, per Blanchard J at para 61, and per Tipping J (who decided the case on a different basis altogether).
41. *Ibid* at para 25. (Anderson J said that he "share[d] the concern expressed by the Chief Justice that the jurisprudence of [*Hosking*] should not be regarded as settled" at para 144.)
42. *Television New Zealand Ltd (TVNZ) v Rogers*, [2007] 1 NZLR 156 (CA) at para 122 [*Rogers CA*].

torts.[43] Tom McKenzie, for example, argues that "the offensiveness test does little analytical work and fails to protect the plaintiff's dignity and should, therefore, be abandoned".[44]

Finally, it should be observed that English courts' support for the high offensiveness test was perhaps not as strong as Gault and Blanchard JJ suggested in *Hosking*. In their discussion of English developments, Gault and Blanchard JJ said that in contrast to breach of confidence (which they said focused on confidential information and did not require a disclosure to be offensive), the emerging English privacy action gave a right of action for the publication of personal information absent an obligation of confidence "but only where that publication is or is likely to be highly offensive to a reasonable person".[45] They continued that in developing this high offensiveness requirement, English courts had drawn upon the US publicity tort. This was because the English Court of Appeal in *Campbell* had referred with approval to Gleeson CJ's dicta in *Lenah* which in turn "comes directly from the American privacy

43. See *e.g.* Lisa Tat, "Plaintiff Culpability and the New Zealand Tort of Invasion of Privacy" (2008) 39:2 Victoria University of Wellington Law Review 365 at 379–80; Chris Hunt, "Breach of Privacy as a Tort" (2014) 1:1 New Zealand Law Journal 286; Chris Hunt, "New Zealand's New Privacy Tort in Comparative Perspective" (2013) 13:1 Oxford University Commonwealth Law Journal 157 at 163–65 [Hunt, "New Privacy Tort"]; Jennifer Moore, "Traumatised Bodies: Towards Corporeality in New Zealand's Privacy Tort Law Involving Accident Survivors" (2011) 24:3 New Zealand Universities Law Review 387 at 402–05; Tim Bain, "The Wrong Tort in the Right Place: Avenues for the Development of Civil Privacy Protections in New Zealand" (2016) 27:2 New Zealand Universities Law Review 295 at 304–05; N A Moreham, "Why is Privacy Important? Privacy, Dignity and the Development of the New Zealand Breach of Privacy Tort" in Jeremy Finn & Stephen Todd, eds, *Law, Liberty and Legislation* (Wellington, NZ: LexisNexis, 2008) 231 at 239 *et seq*; N A Moreham, "Recognising privacy in England and New Zealand" (2004) 63:3 Cambridge Law Journal 527 at 555–58.

44. Thomas Levy McKenzie, "The New Intrusion Tort: The News Media Exposed?" (2014) 45:1 Victoria University of Wellington Law Review 79 at 95.

45. *Hosking*, *supra* note 4 at para 42.

jurisprudence".[46] This conclusion influenced Gault and Blanchard JJ's adoption of the high offensiveness test. Just before setting out their own version of the two-part privacy test, they said that its requirements were "a logical development of the attributes identified in the United States jurisprudence and adverted to in judgments in the British cases".[47]

All of these conclusions seem to have been based on the fact that the high offensiveness test had been applied by the English Court of Appeal in *Campbell* in 2002. But the Court's approach in that case was inconsistent with another leading English Court of Appeal decision, *A v B Plc*,[48] in which Lord Woolf CJ identified the plaintiff's reasonable expectation of privacy as the gravamen of liability and did not adopt a highly offensive requirement at all.[49] Further, in one of the pre-*Hosking* iterations of *Douglas v Hello! Ltd* litigation,[50] Justice Lindsay had declined to rely on the high offensiveness test developed in *Campbell CA*[51] to determine whether surreptitiously taken photographs of the plaintiffs' wedding reception should be regarded as confidential. He noted in doing so that Gleeson CJ's dictum "does not even purport to be an exclusive definition of what is private".[52]

It is unsurprising, then, that just two months after the *Hosking* case

46. *Ibid* at para 43.
47. *Ibid* at para 117.
48. [2002] EWCA Civ 337.
49. *Ibid* at para 11ix-x. (Although the Court in *A v B Plc* cited the passage in which Gleeson CJ expresses support for the high offensiveness test in *Lenah*, *supra* note 8, this was simply to show "the difficulty of distinguishing between public and private information" and not to endorse the high offensive test as a means of determining what is private at para 11vii.)
50. [2003] EWHC 786 (Ch) [*Douglas*]. (This litigation concerned the publication of unauthorised photographs of the wedding of celebrity actors, Michael Douglas and Catherine Zeta-Jones.)
51. *Campbell CA*, *supra*, note 16.
52. *Douglas*, *supra* note 50 at paras 188–92. (He continues that the fact that "matters the disclosure of which would be highly offensive to a reasonable person of ordinary sensibilities may, on that account, be regarded as private does not, of itself, suggest that no other matters can be so regarded" at para 191.)

was decided, the high offensiveness requirement was rejected by the House of Lords in *Campbell* in favour of the reasonable expectation of privacy test. The majority also overturned the Court of Appeal's decision that the plaintiff was not entitled to damages for publication of the details of her drug addiction treatment and photographs of her leaving a Narcotics Anonymous meeting. In what has emerged as the leading judgment in that decision, Lord Nicholls said that "the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy" and that the high offensiveness test had no place in it.[53] Baroness Hale agreed. Lord Carswell concurred with the judgments of both Baroness Hale and Lord Hope (who was in favour of relying on a "substantial" offensiveness test in cases where whether the information is public or private is not "obvious")[54] but decided the case on the basis of the intimate nature of the information, making it "not necessary" to consider the high offensiveness part of the test.[55] This led the English Court of Appeal to say in *Associated Newspapers Ltd v HRH Prince of Wales*[56] that Gault and Blanchard JJ's claim in *Hosking* that a plaintiff could only recover under the English privacy tort if publication is or was likely to be highly offensive to a reasonable person did not reflect the law as it stood in 2006.[57] It is perhaps also questionable whether it was a sufficiently fulsome articulation of the law as it stood in 2004.

The failure to recognise the alternative test in *A v B Plc* (and the subsequent adoption of that test by the House of Lords in *Campbell*) reduces the weight that should be given to Gault and Blanchard JJ's decision to include it in the New Zealand privacy tort. It not only means that an important alternative approach (*i.e.* one based principally on reasonable expectations of privacy) was not considered in *Hosking* but that consistency with English law — which Gault and Blanchard JJ themselves regarded as desirable — was not achieved. In those circumstances, it is regrettable that greater consideration was not given

53. *Campbell HL*, *supra* note 3 at para 21.
54. *Ibid* at para 92.
55. *Ibid* at para 166.
56. [2006] EWCA Civ 1776.
57. *Ibid* at para 65.

to the significant constitutional and cultural differences between New Zealand and the United States, particularly in respect of the protection of freedom of expression.

IV. Why The High Offensiveness Test Should Be Abandoned

All these reservations about the high offensiveness test are, it is suggested, rightly held. Indeed, this section will set out three main reasons why New Zealand courts should abandon it. First, the absence of clear principle about the operation of the high offensiveness test makes it unacceptably unpredictable. Second, when courts have set out principles to guide the application of the test, they have taken too narrow a view of the harm caused by privacy breaches. This in turn obfuscates the dignity and autonomy interests at the heart of the privacy action. Third, all of the tools needed to exclude unmeritorious claims are already available under the reasonable expectation of privacy test. The high offensiveness test is therefore unnecessary.

A. Lack of Principle in the Application of the High Offensiveness Test

The first problem with the New Zealand high offensiveness test is the lack of clear principle in the jurisprudence about how it should be applied. In fact, in some cases, the question of whether the intrusion or publicity is highly offensive is disposed of with no reasoning at all. For example, in the strike-out decision in *Henderson v Slevin*,[58] Associate Justice Osborne gave no reasons for his conclusion that a reasonable person would not think it highly offensive for a liquidator to pass on the plaintiff's computer records to an enforcement unit nor to examine them himself.[59] He just said that the requirement was not satisfied. Similarly, in declining an application for an interim injunction in *Clague v APN News and Media Ltd*,[60] Justice Toogood gave no reasons for his conclusion that,

58. [2015] NZHC 366.
59. *Ibid* at paras 48, 71.
60. [2012] NZHC 2898.

although it would be embarrassing to the plaintiff and distressing to the plaintiff and his family, he was not persuaded that publicity around a police investigation into allegations of domestic assault would be highly offensive or objectionable to a reasonable person.[61]

In other cases, courts have set out potentially useful principles for the application of the high offensiveness test but then failed clearly to apply them to the facts, instead treating the matter as a question of judicial instinct. For example, when determining whether the high offensiveness test was met on the facts in *Hosking*, Gault and Blanchard JJ simply said that:

> We are not convinced a person of ordinary sensibilities would find the publication of these photographs highly offensive or objectionable even bearing in mind that young children are involved. … The real issue is whether publicising the content of the photographs (or the 'fact' that is being given publicity) would be offensive to the ordinary person. We cannot see any real harm in it.[62]

There is nothing in their discussion to explain why the proposed publication was insufficiently harmful — was it, for example, because the children were unaware of it, because they were too young to suffer distress, or because the information in the photograph had already been held not to be private? The leading intrusion case, *Holland*, is similar. Whata J begins the judgment by usefully saying that the offensiveness element is "a question of fact according to social conventions or expectations"[63] and by citing a passage identifying "various factors" which will bear on whether an intrusion is "highly offensive" including "the degree of intrusion, context, conduct and circumstances of the intrusion, the motive and objectives of the intruder and the expectations of those whose privacy is invaded".[64] But when it comes to applying the high offensiveness test, he does not apply those factors systematically to the facts. Rather, he simply says that the defendant's act of filming the plaintiff in the shower was

61. *Ibid* at para 38.
62. *Hosking*, *supra* note 4 at para 165.
63. *Holland*, *supra* note 24 at para 16.
64. *Ibid* citing *Miller v National Broadcasting Co*, 187 Cal App (3d) 1463 (Cal Ct App (US) 1986) at 1483 [*Miller*] and citing *Jones*, *supra* note 30 at para 58.

offensive without saying why.[65]

Faesenkleot v Jenkin is an exception to this trend. In that case, the plaintiff sought an injunction to prevent his neighbour, with whom he was already engaged in an acrimonious dispute, from filming people using the plaintiff's driveway. Justice Asher expressly identifies and applies the principle that a deliberate intrusion which was designed to offend the plaintiff "might be more offensive than one which is obviously accidental and incidental to another purpose",[66] concluding that the camera in that case was not installed with the purpose of offending the plaintiff.[67] He also said that the greater the expectation of privacy interfered with by the intrusion, "the more likely an intrusion will be offensive",[68] concluding that the surveillance was not offensive because the area surveyed was not large nor used for any intimate purpose, the camera did not film the plaintiff's home or garden, and because cars and pedestrians could still use the driveway without being caught by the camera.[69] Although this more detailed reasoning is welcome, the broad principles applied in this case still provide only limited guidance for future cases (especially since Asher J had already decided that the plaintiff had no reasonable expectation of privacy in respect of the filming (in part because the plaintiff was in fact

65. *Holland*, *ibid* at para 99. (In a similar vein, in the pre-*Hosking* case of *P v D*, *supra* note 6, Nicholson J said that offensiveness has to be assessed from the perspective of a person of ordinary sensibilities "in the same position" as the plaintiff at para 39 and that courts should not take an idealistic view about societal attitudes to mental illness at para 37, but when it came to applying the law to the facts, he simply held that he accepted that the plaintiff had the "stated feelings" and that "a reasonable person of ordinary sensibilities would in the circumstances also find publication of information that they had been a patient in a psychiatric hospital highly offensive" at para 39.)
66. *Faesenkloet*, *supra* note 23 at para 47.
67. *Ibid* at paras 47–49.
68. *Ibid* at para 50.
69. *Ibid*. (Asher J concluded that the plaintiff did not have a reasonable expectation of privacy in respect of the filming for similar reasons at paras 44–45.)

able to evade the camera's gaze altogether)).[70]

The general paucity of reasoning about the application of the high offensiveness test makes its operation unpredictable. Although a test appealing to a judge's instincts might be useful for disposing of unmeritorious cases once they come to court, it does not delineate the boundaries of the privacy torts clearly. This in turn makes it difficult for people — including those seeking to publish information, investigate wrongdoing or advise clients wanting to do these things — to know exactly what the law does and does not proscribe. This level of uncertainty is undesirable. Although privacy actions need to retain a degree of flexibility to reflect legitimate differences in the degree of inaccessibility that each individual seeks, they do not need to be imprecise or unpredictable. Indeed, given that the action has the potential to stymie freedom of expression and prevent legitimate investigation of wrongdoing, it is important that they are not. The application of the high offensiveness test requires more, then, than a general conclusion at the end of the judgment about whether or not the judge in a particular instance thought that the behaviour was offensive.

It is important to note at this point that this lack of clear reasoning in the New Zealand privacy case law is a particular feature of the application of the high offensiveness part of the privacy tests. The principles governing the application of the reasonable expectation of privacy test are, in contrast, much better articulated.[71] As outlined above, when it comes to applying the reasonable expectation of privacy test in *Hosking*, Gault and Blanchard JJ explain that information about health, personal relationships, and finances "may be easy to identify as private" and that reasonable expectations of privacy depend on what people applying "contemporary standards of morals and behaviour, would understand to

70. *Ibid* at para 50.

71. It should be noted that there is also still uncertainty about the scope of the requirement in *Holland* that the plaintiff establish an "intentional and unauthorised intrusion" into "seclusion (namely intimate personal activity, space or affairs)" in the intrusion tort. See further N A Moreham, "A Conceptual Framework for the New Zealand Tort of Intrusion" (2016) 47:2 Victoria University of Wellington Law Review 283.

be meant to be unobserved".[72] They also discussed in some detail the impact that a plaintiff's location and public profile — including that of involuntary public figures, like the children at issue in that case — would have on his or her reasonable expectations of privacy.[73]

The factors which bear on the application of the reasonable expectation of privacy test are even better articulated in England and Wales. In the influential judgment of the Court of Appeal in *Murray v Express Newspapers Plc*,[74] Sir Anthony Clarke MR said (in the course of holding that the young son of well-known author J K Rowling could restrain the defendants from publishing photographs taken of him on the public street during a family trip to a café):

> As we see it, the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include the attributes of the claimant, the nature of the activity in which the plaintiff was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came into the hands of the publisher.[75]

These factors were systematically applied in *Murray* itself and have been adopted in numerous first instance and appellate judgments since.[76] This has in turn led to the emergence of identifiable principles governing the application of the reasonable expectation of privacy test. Indeed, this author has argued elsewhere that it is now possible to identify from within English law both high-level principles governing the application of the reasonable expectation of privacy test and specific categories of

---

72. *Hosking*, *supra* note 4 at para 119 citing *Lenah*, *supra* note 8 at para 42.
73. *Ibid* at paras 120–24.
74. [2008] EWCA Civ 446 [*Murray*].
75. *Ibid* at para 36. (The Court also expressly rejected the *Hosking* court's approach to the children of public figures on the basis that it put too little weight on the children's separate privacy interests at para 51.)
76. See *e.g. Weller v Associated Press Ltd*, [2015] EWCA Civ 1176 at para 16; *Re JR38*, [2015] UKSC 42 at para 98.

information that are likely to satisfy it.[77] The reasonable expectation of privacy test is therefore applied in a much more principled way than the high offensiveness test.

B. Taking Too Narrow a View of Privacy Harms

One notable exception to the lack of principle in the application of the high offensiveness test in New Zealand is the approach taken in *Andrews v Television New Zealand*.[78] Regrettably, however, that case is problematic for other reasons.

Andrews concerned a reality television programme which showed in considerable detail the two plaintiffs being extricated from a car wreck on the side of the road late one night. The footage included intimate conversations between the couple including exchanges in which Mrs Andrews told her injured husband that she loved him and asked him to "stay with her". The couple were not informed of the filming; instead, they first learnt of it some months later when the programme appeared on television during a party at a neighbour's house.

In his decision rejecting the couple's claim for damages, Justice Allan accepted that the couple had a reasonable expectation of privacy in respect of the broadcast of intimate conversations between them but said

77. See further N A Moreham, "Unpacking The Reasonable Expectation Of Privacy Test" 134 Law Quarterly Review [forthcoming in 2018] [Moreham, "Unpacking"]. (This article argues that under the first of the two high-level principles, courts consider whether recognition of a reasonable expectation of privacy is consistent with societal attitudes to the information or activity and under the second, they ask whether the plaintiff relied on socially-recognised signals to show that he or she regarded the information or activity as private. Categories of information or activity which society will usually regard as private include matters relating to the appearance or workings of the physical body, to sexual encounters or activity, to the intimate details of one's personal relationships, and the intimacies of one's family and/or domestic life.)

78. *Andrews*, *supra* note 23.

that the broadcast was not highly offensive.[79] In reaching that conclusion, he focused on the tone of the publicity. He held that:

> There may be instances where the disclosure of otherwise relatively inoffensive facts may become offensive by reason of the extent and tone of a publication. So the manner of disclosure is a relevant consideration.[80]

Later in the judgment, Allan J said that there was nothing in the programme which showed the couple in "a bad light".[81] He said that neither plaintiff was able to point to anything about the programme which they regarded as humiliating, embarrassing, or offensive and noted that it had not made mention of the fact that both plaintiffs had excess blood alcohol levels at the time of the accident.[82] Mrs Andrews had accepted, he said, that she was portrayed as "a caring person, very much concerned about her husband's wellbeing" and "coping well by making light of the situation" and that nothing which she had said to her husband could be regarded as humiliating or embarrassing to either of them.[83] Although Allan J said that the absence of inherently embarrassing material "does not lead inexorably to the conclusion that the disclosure was not humiliating and distressful",[84] it therefore clearly had a significant bearing on his disposal of the case.

This approach, with respect, misses the point. The publicity tort is not about protection from reputational harm or embarrassment but the preservation of choice about when the private aspects of one's life will be accessible to others. This, as widely recognised by commentators and

---

79. *Ibid* at para 100. (Allan J also held that had the plaintiffs established that the footage had breached their privacy, it would have been outweighed by a legitimate public concern in the activities of emergency services at para 91.)
80. *Ibid* at para 51.
81. *Ibid* at para 67.
82. *Ibid* at para 67. (They had both escaped conviction for drunk driving because the police were unable to establish which of them had been driving.)
83. *Ibid* at para 68.
84. *Ibid* at para 69.

judges, is a fundamental aspect of individual dignity and autonomy.[85] The complaint in *Andrews* is therefore not that the footage made the couple look bad but that someone else decided that the world should see and hear them during that traumatic rescue. This is humiliating and distressful in itself regardless of the tone of the documentary.[86] Other examples drive home that point. Is it really alright, for example, to broadcast surreptitiously obtained footage of a father comforting his dying child in hospital because it makes him look like a caring person? And what say there is widespread agreement that the plaintiff looks great in naked photographs that her ex-boyfriend put up on the internet? Clearly that does not mean that they are no longer humiliating. The objection in these situations is that it should be the subjects themselves — not the defendants — determining whether these intimate matters are shown. By suggesting that the unwanted broadcast of detailed footage of the event has to be in some way negative or embarrassing, *Andrews* therefore obfuscates what the privacy action is really about.

It should also be noted that Allan J's conclusion runs contrary to an increasing body of evidence showing the harm caused by unwanted exposure at intimate or traumatic times, even if the coverage is positive. For example, friends and family members of the men who died in the Pike River mine disaster in 2011 have said that intense media intrusion

---

85. See *e.g.* Edward J Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39:6 New York University Law Review 962; Stanley Benn, "Privacy, Freedom and Respect for Persons" in James Roland Pennock & John W Chapman, eds, *Privacy*, *NOMOS XIII* (New York: Atherton Press, 1971) 1; David Feldman, "Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty" (1994) 47:2 Current Legal Problems 41; Ruth Gavison, "Privacy and the Limits of the Law" (1980) 89:3 Yale Law Journal 421; Alan Westin, *Privacy and Freedom* (New York: Antheneum, 1967); *Pavesich v New England Life Insurance Co*, 50 SE 68 at 70 (Sup Ct Ga (US) 1905); *Hosking*, *supra* note 4 at para 239, per Tipping J; *Campbell HL*, *supra* note 3 at para 50, per Lord Hoffman.

86. See generally Catlin Wilson & Daniel Nilsson, "Protecting Our Personal Sphere" (2013) 1:1 New Zealand Law Journal 8 at 9–10; Tat, *supra* note 43 at 379; Moreham, "Why is Privacy", *supra* note 43 at 240–43.

in the days following the explosion left them feeling "violated", physically unsafe, and commodified.[87] The fact that the coverage was sympathetic did not alter the strength of any of these reactions.

In *Andrews*, Allan J was of the view that Gault and Blanchard JJ's decision in *Hosking* required him to take this narrow, tone-focused approach to the highly offensive requirement. He said, when dismissing Tipping J's view in *Hosking* that the reasonable expectation and high offensiveness requirements would "be likely to coalesce",[88] that it was important to bear in mind "as a matter of analysis at a practical level that the 'highly offensive' test relates to publicity" and is therefore not part of the test of whether information is private.[89] The court "does not reach the stage of considering the highly offensive test unless and until it has concluded that what has been disclosed was private information".[90] In his view, then, the focus on the nature of the publicity flowed from Gault and Blanchard JJ's formulation of the privacy test.

The highly offensive publicity test does certainly point away from the conclusion — which the English Court of Appeal recently reached in *Gulati v MGN Ltd*[91] — that breach of privacy without more can cause compensable harm. Rather, its inclusion implies that even if the breach of privacy is sufficiently serious to be regarded as socially unacceptable (as the reasonable expectation of privacy test requires) it still might not cause real humiliation, distress, or other harm to the plaintiff. Something more, it says, is needed. The test therefore obscures the fact that all privacy interferences "humiliate" their subjects — and undermine their dignity and autonomy — by shifting control over something personal to

87. N A Moreham & Yvette Tinsley, "Media Intrusion into Grief: Lessons from the Pike River Mining Disaster" in Andrew T Kenyon, ed, *Comparative Defamation and Privacy Law* (Cambridge: Cambridge University Press, 2016) 115 at 127 [Moreham & Tinsley, "Media Intrusion into Grief"].

88. *Andrews*, *supra* note 23 at para 25 (citing *Hosking*, *supra* note 4 at para 256).

89. *Ibid*.

90. *Ibid*.

91. [2015] EWCA Civ 1291. (Substantial damages were awarded in that case for the loss of privacy itself even in the absence of distress or other harm.)

the subject to someone other than the subject.[92]

This obfuscation is exacerbated by the fact that the high offensiveness element of Gault and Blanchard JJ's test requires the plaintiff to show that the publicity would cause a reasonable person "offence". The word "offensive" is usually used to refer to something which is insulting or denigrating in some way — an opinion which is racist or sexist, for example. This is not the language of privacy. In privacy situations, people use the language of dignity and autonomy: "violation", lack of respect, commodification.[93] The word "offensiveness" therefore distracts from the interests at the core of the privacy right.

All this makes it less surprising that the judge in *Andrews* focused on the lack of denigration or criticism in the broadcast of the couple rather than the humiliation inherent in it. It also suggests that at the very least the high offensiveness test should be reformulated to reflect Gault and Blanchard JJ's actual concern in *Hosking*, namely that the publicity be "truly humiliating and distressful"[94] to an objective, reasonable person.[95]

---

92. Hyman Gross, "Privacy and Autonomy" in James Roland Pennock & John W Chapman, eds, *NOMOS XIII* (New York: Atherton Press, 1971) 169 at 169, 177. (He continues that public disclosures of private facts always result in the individual being shamed, not because of what others learn about him or her, but because someone other than the victim is determining what will be done with what is learnt at 177.) In *Hosking*, *supra* note 4 at para 125 Gault and Blanchard JJ also implicitly acknowledge this by saying that "[i]n theory a rights-based cause of action would be made out by proof of breach of the right irrespective of the seriousness breach" (but they go on to say that such an approach is unrealistic and that the high offensiveness test is therefore needed at para 127).
93. Moreham & Tinsley, "Media Intrusion into Grief", *supra* note 87; UK, The Leveson Inquiry, *An Inquiry into the Culture, Practices and Ethics of the Press: Report*, by The Right Honourable Lord Justice Leveson, vol 2 (London: The Stationery Office, 2012) at 504 para 3.2, 540 paras 1.7, 1.10, 548 para 3.4, 553 para 3.27, 602 para 2.44 (where Sir Brian Leveson spoke of individual lives being treated like "commodities" by the media).
94. *Hosking*, *supra* note 4 at para 126.
95. *Ibid* at para 117.

But even given its current formulation, Allan J's application of the high offensiveness test in *Andrews* is too narrow. Although Gault and Blanchard JJ argued in *Hosking* that the high offensiveness test was necessary to exclude non-serious claims from the reach of the action, neither suggested that the "tone" of the publicity would determine whether it was satisfied. Rather, they focused on whether the publicity was widespread and would cause a reasonable plaintiff distress. And, contrary to Allan J's suggestion, Tipping J's point in *Hosking* (echoed by Young P in *Rogers CA*)[96] about the reasonable expectation of privacy and high offensiveness tests usually coalescing can be reconciled with the view that it is the publicity which has to be offensive. What Tipping J and Young P said in those cases is that offensiveness — whether it is of the publicity or anything else — should inevitably follow interference with a reasonable expectation of privacy.

The second reason why Allan J concluded that the high offensiveness test was not satisfied in *Andrews* was that that the couple did not get upset about the right thing in the right way. Allan J said that, as the evidence unfolded, it emerged that "it was not the intrusion on the plaintiffs' privacy which lay at the heart of the proceeding" but rather their "chagrin and annoyance" at not being told about the filming or the broadcast.[97] "Even more" important was the fact that the plaintiffs were given no prior notice of the date of the broadcast and as a result found themselves watching the broadcast for the first time in the company of strangers.[98] But all this, says Allan J, is immaterial because "a failure to obtain consent prior to publication is not an ingredient of the tort of breach of privacy".[99] Further, consent is not normally sought by broadcasters if the filming takes place in public view.[100] It followed, he said, that given that neither plaintiff found the broadcast of conversations at the accident scene as highly offensive, it was impossible to conclude that a reasonable person

96. *Rogers CA*, *supra* note 42.
97. *Andrews*, *supra* note 23 at para 69.
98. *Ibid*.
99. *Ibid* at para 70.
100. *Ibid*.

in the shoes of the plaintiffs would do so.[101]

This reasoning is, with respect, difficult to follow. First, considering whether broadcasters normally seek consent before broadcasting footage of something which was in public view begs the very question the proceedings were designed to answer. The whole point of this case is to determine whether broadcasters *should* be entitled to publish footage of this nature without informing or asking its subjects.[102] What the media usually do should not be determinative of this matter. Further, contrary to Allan J's contention, questions of choice and consent are central to the right to privacy including in the tort of giving publicity to private facts. As Tipping J said in *Hosking*, privacy is all about "the right to have people leave you alone if you do not want some aspect of your private life to become public property … that some aspects of people's lives should be able to remain private if they so wish".[103] Consent — or lack thereof — plainly lies at the heart of these ideas of "wanting", "wishing", and "choosing". The fact that the plaintiffs were upset that their consent was not sought is therefore entirely relevant to their claim.

Third, it is difficult to see why the plaintiffs' "chagrin and annoyance" were not enough to satisfy the requirement that the privacy interference causes real humiliation, distress, or other harm. It is clear from Allan J's own findings of fact that the plaintiffs were deeply affected by the defendant's conduct. He held that:

> The plaintiffs were greatly distressed by the screening of the programme. They had no warning of it. The accident had given rise to tensions within the family, particularly in the relationship between the plaintiffs themselves and in respect of the emotional health of one of their children. They were forced to re-live the trauma of the accident, as they saw the scene from an entirely different viewpoint. Moreover, all of this occurred while in the company of a number of other people, not all of whom were known to them.[104]

---

101. *Ibid* at para 71. (Even on its face, this statement is questionable. If the highly offensive publicity test is truly objective, then a plaintiff's unusually thick skin about a privacy intrusion should be no more relevant that another plaintiff's thin one.)
102. *Ibid* at para 70.
103. *Hosking*, *supra* note 4 at paras 238–39.
104. *Andrews*, *supra* note 23 at para 15.

This is exactly the kind of distress and consequential harm that was described by Gault and Blanchard JJ in *Hosking*.[105] People experience a range of emotions at having their privacy interfered with including "chagrin and annoyance". It is not at all clear why only certain of these negative emotions should satisfy the high offensiveness test.

It is unsurprising in light of all this that *Andrews* has been the subject of much academic criticism.[106] Not only did it deny a remedy to the meritorious (albeit perhaps unsympathetic) plaintiffs in that case, it misinterpreted the nature of privacy harms and provided a carte blanche for voyeurs and media companies to broadcast footage of victims at will. The decision in *Andrews* sets the bar for recovery both too high and in the wrong place. By doing so, it fortifies arguments for abandoning the high offensiveness test itself.

C. The High Offensiveness Test is Unnecessary

This leads to the final reason for abandoning the high offensiveness test — it is unnecessary. It will be recalled that in *Hosking*, Gault and Blanchard JJ said that they included the high offensiveness requirement because they believed that it is necessary to keep the action within bounds. It is "quite unrealistic", they said, to contemplate legal liability for all publications of private information: it would be "absurd", for example, "to consider actionable merely informing a neighbour that one's spouse has a cold".[107] This is not doubted. Privacy torts have the potential both to silence legitimate speech and to deter the desirable investigation of wrongdoing. They therefore need to be kept within clearly defined parameters. Courts do not, however, need to rely on the high offensiveness test to do this.

105. *Hosking*, *supra* note 4 at para 126. (Indeed, since, as discussed above, "offence" imports an idea of denigration or insult, "chagrin and annoyance" seem to fit particularly comfortably within the concept.)
106. See Moore, *supra* note 43 at 402–05; McKenzie, *supra* note 44 at 95–97; Ursula Cheer, "The Future of Privacy: Recent Legal Developments New Zealand" (2007) 13:2 Canterbury Law Review 169 at 183–85; Bain, *supra* note 43 at 319–22; Tat, *supra* note 43 at 379–80; Moreham, "Why is Privacy", *supra* note 43 at 240–43.
107. *Hosking*, *supra* note 4 at para 125.

This is because unmeritorious claims are already excluded from the privacy tort through the proper operation of the reasonable expectation of privacy test.

All three of the majority judges in *Hosking* made it clear that the reasonable expectation of privacy test will not be satisfied unless the plaintiff's privacy expectations accord with general societal standards. As Tipping J says, the word "reasonableness" plainly imports into the privacy tort an enquiry into "contemporary societal values" in respect of the matter at hand.[108] Gault and Blanchard JJ also approved of Gleeson CJ's observation in *Lenah* that "contemporary standards of morals and behaviour" determine what is and is not private[109] and in *Holland*, Whata J stressed (citing the Californian Supreme Court case of *Shulman v Group W Productions*) that in order to establish a reasonable expectation of privacy, the plaintiff must show both that he or she had a subjective expectation of solitude or seclusion and that that expectation was "objectively reasonable".[110] All this means that whether a plaintiff has a reasonable expectation of privacy is a *normative* enquiry into what privacy protection a plaintiff can expect the law to provide.[111] Once this is recognised, it becomes plain that it will not be satisfied unless the interference in question is a serious one. The plaintiff has to show that normal everyday people would share their view that the information or activity is private and should be legally protected. This will not be the case if your spouse tells your neighbour — or anyone else for that matter — that you have a cold.

The superfluousness of the high offensiveness test is reinforced when one considers the factors which Whata J identified in *Holland* as relevant to the application of the high offensiveness test. It will be recalled that in *Holland*, Whata J (drawing on *Jones v Tsige* and *Miller v National Broadcasting Co*) said that "various factors" will bear on whether an intrusion is "highly offensive" including "the degree of intrusion,

108. *Ibid* at para 250.
109. *Ibid* at para 119 citing *Lenah*, *supra* note 8 at para 42.
110. *Holland*, *supra* note 24 at para 17 citing, inter alia, *Shulman*, *supra* note 30 at para 490.
111. See further, Moreham, "Unpacking", *supra* note 77.

context, conduct and circumstances of the intrusion, the motive and objectives of the intruder and the expectations of those whose privacy is invaded".[112] But these factors have all also been identified by the English Court of Appeal in *Murray* as relevant to the application of the reasonable expectation of privacy test (noting that English and New Zealand law are very similar in this regard).[113] In fact, there is complete overlap between the two tests. To take the elements one-by-one, the *Holland* enquiries into the "degree", "conduct", and "circumstances"[114] of the intrusion align with the *Murray* enquiry into "the nature and purpose of the intrusion",[115] the *Holland* enquiry into "context"[116] aligns with the *Murray* court's consideration of the attributes of the plaintiffs, the nature of the activity which they were engaged, the place at which the relevant activity was happening, the absence of consent and the circumstances in which the information came into the publisher,[117] *Holland*'s concern with "the motives and objectives of the intruder"[118] is covered by the *Murray* enquiry into "the purposes for which the information came into the hands of the publisher",[119] and finally, the concern in *Holland* with the "expectations of those whose privacy is invaded"[120] plainly overlaps with the reasonable expectation of privacy test itself. It is difficult to see, then, what tools the high offensiveness test is providing that are not already part of the reasonable expectation of privacy test.

It should be recalled at this point that English courts determine privacy claims simply by applying a reasonable expectation of privacy test and a public interest defence. The high offensiveness test was expressly rejected by the House of Lords in *Campbell*. In that case, Baroness Hale

112. *Holland*, *supra* note 24 at para 16 citing *Miller*, *supra* note 64 at 1483 and *Jones*, *supra* note 30 at para 58.
113. For discussion of the factors which the *Hosking* majority regarded as relevant to the reasonable expectation of privacy test see Part II.
114. *Holland*, *supra* note 24 at para 16.
115. *Murray*, *supra* note 74 at para 36.
116. *Holland*, *supra* note 24 at para 16.
117. *Murray*, *supra* note 74 at para 36.
118. *Holland*, *supra* note 24 at para 16.
119. *Murray*, *supra* note 74 at para 36.
120. *Holland*, *supra* note 24 at para 16.

held that "an objective reasonable expectation test is much simpler and clearer" than one which asks whether "disclosure or observation would be highly offensive to a reasonable person of ordinary sensibilities".[121] Lord Nicholls agreed saying that the "highly offensive" phrase was "suggestive of a stricter test of private information than a reasonable expectation of privacy" and second, that it can:

> all too easily bring into account, when deciding whether the disclosed information was private, considerations which go more properly to issues of proportionality; for instance, the degree of intrusion into private life, and the extent to which the publication was a matter of proper public concern.[122]

Reinforcing all this, the English Court of Appeal recently held that the first instance judge in a judicial review decision was wrong to apply Lord Hope's high offensiveness test to determine whether information about the plaintiffs' indebtedness to the National Health Service was private and confidential at common law. Lord Neuberger MR said, speaking for the Court in *W, X, Y and Z v Secretary of State for Health*,[123] that "in so far as the judge regarded 'highly offensive' formulation as material to whether the information was private and confidential, he was wrong to do so".[124]

V. Conclusion

If English courts can rely solely on the reasonable expectation of privacy test and legitimate public concern defence to dispose of the dozens of privacy cases which come before them each year, the New Zealand courts can too. Such an approach would move New Zealand courts away from reliance on the imprecise and often value-laden high offensiveness requirement and onto an element which is increasingly the subject of detailed and principled reasoning both in New Zealand and abroad. Unmeritorious claims can easily be dealt with on a reasonable expectations-based approach — non-serious cases will not satisfy the reasonableness test. Indeed, the need to deal with unmeritorious claims

121. *Campbell HL*, *supra* note 3 at para 135 citing *Lenah*, *supra* note 8.
122. *Campbell HL*, *ibid* at para 22.
123. [2015] EWCA Civ 1034.
124. *Ibid* at para 34. (The appeal was ultimately dismissed on other grounds.)

under the reasonable expectation of privacy test would encourage the more nuanced development of that requirement in New Zealand law.

Whilst it is difficult to see what value the high offensiveness test adds to the New Zealand privacy torts, it is not difficult to see what it might be taking away. As discussed, lack of clarity about what is and is not offensive undermines the predictability of the New Zealand privacy actions as a whole. And the narrow types of harm which some courts (most notably the High Court in *Andrews*) say will cause "offence" obfuscates the interests in dignity and autonomy at the heart of the privacy action. The high bar set by the high offensiveness requirement also seems to have arrested the general development of the torts. In the 14 years since *Hosking* was decided, only four successful privacy claims have been brought in New Zealand.[125] In contrast, courts in England and Wales have considered many dozens of cases and awarded relief to a wide range of plaintiffs. Some of these differences can be put down to the different context in which the torts are operating (including the larger number of celebrities living in the United Kingdom and the media's strong appetite for stories about them) but there is every reason to think that the higher bar for recovery under the New Zealand torts (particularly under the high offensiveness test) is a factor.

---

125. See respectively, *Holland*, *supra* note 24; *A v Fairfax New Zealand Ltd*, [2011] NZHC 71 (in which it was held that the fact that the plaintiff had made a sex offence complaint was private); *JJC v Fairfax New Zealand Ltd*, HC Auckland CIV-2001-404-5605 (where the fact that the plaintiff was a child whose mother was allegedly murdered by his father was private); *Brown*, *supra* note 23 (police breached privacy by distributing a flier identifying the plaintiff (by full name and photograph) as a convicted paedophile living in the area). There were also three successful claims which predated *Hosking*: *P v D*, *supra* note 6 (in which a public figure obtained an injunction restraining publication of an article about his or her mental health); *L v G*, [2002] NZAR 495 (DC) (regarding non-consensual publication of an unidentifiable woman's genitalia in an adult lifestyles magazine); *Tucker*, *supra* note 6 (regarding the proposed disclosure of the fact that a man seeking to raise funds for heart surgery was a convicted paedophile).

Many New Zealand judges have indicated a willingness to reconsider the formulation of the requirements of the privacy torts in an appropriate case. It is hoped that when the opportunity presents itself, the high offensiveness test will be abandoned.

Regulating Surveillance: Suggestions for a Possible Way Forward

Moira Paterson*

The need for privacy protection against surveillance has assumed new significance due to the onslaught of technological developments that increasingly undermine the capacity of individuals to maintain anonymity in relation to public activities and their physical movements across public places. Modern surveillance practices arguably require a rethinking of some of the tests and assumptions that underlie existing privacy laws, including tests based on "reasonable expectations of privacy", distinctions between content and between transactional data and content. They also call for active consideration of the full range of regulatory tools available and ways in which those tools can be adapted to reduce their existing limitations. This paper draws on a range of privacy resources, and on regulatory theory more generally, to suggest possible ways forward.

* Professor of Law, Monash University. Early drafts of this article were presented at the Privacy Law Scholars Conference at the George Washington School of Law on 6 June 2014 and at the Law & Technology Workshop at Tel Aviv University on 5 December 2016. I wish to record my thanks for the valuable feedback received at each of these events.

I. Introduction
II. The Problem of Privacy in Public Places
III. Why Loss of Anonymity Requires Attention
IV. Existing Regulatory Frameworks and their Shortcomings
A. Telecommunications Interception Laws
B. Surveillance Device Laws: Listening Devices and Beyond
C. Common Law and Statutory Rights of Action for Breaches of Privacy
D. Data Protection Laws and Other Laws Based on Fair Information Practices ("FIPs")
V. The Significance of Constitutional/Human Rights Frameworks
VI. Insights from Regulatory Theory
VII. A Suggested Way Forward

I. Introduction

The need for privacy protection against surveillance has assumed new significance due to the onslaught of technological developments that increasingly undermine the capacity of individuals to maintain anonymity in relation to public activities and their physical movements across public places. Two examples are illustrative of this trend.

The first is the FaceSDK application, which is advertised as enabling developers using a variety of computing languages to build platforms based on face recognition. This is described as being "used in hundreds of applications for identifying and authenticating users with webcams, looking up matching faces in photo databases, automatically detecting facial features in graphic editors, and detecting faces on still images and video streams in real-time".[1]

The second is a recently developed "IMSI catcher" device, which is described as "a low-cost way to discover the precise location of

1. See Luxand Inc, "Detect and Recognize Faces with Luxand FaceSDK" *Luxand*, online: Luxand <https://www.luxand.com/facesdk/>.

smartphones using the latest LTE standard[2] for mobile networks"[3] and as being able to "track users for days with little indication anything is amiss".[4]

What is significant about technologies of this type is that they make it increasingly easy to extract or infer identity from non-identifying signs and information. This amounts to an unprecedented assault on anonymity, making it increasingly difficult for individuals, other than hermits, to go about their lives beyond the reach of others. More specifically, these technologies make it difficult for individuals to keep at bay the uncalled for reactions and consequences that result from being known to and accessible by random and unknown individuals and entities who use the aforementioned devices and applications.

The implications of technology-assisted surveillance activities have, to date, been considered most closely in the context of surveillance by law enforcement and national security bodies. They have also received some scrutiny in the online context. However, it is arguable that there is also a need to regulate surveillance more generally, especially as it relates to public places.

Across the board surveillance is important because surveillance and the possible privacy harm to which it may give rise are no longer solely the main provinces of law enforcement and national security bodies; surveillance now underlies many of the decision-making processes of businesses in relation to current and prospective customers and employees, and it is increasingly within the reach of private individuals as discussed below. The regulation of surveillance more generally is also important because of the erosion of the boundaries between public

2. The Long Term Evaluation Standard is a 4G mobile communications standard for high-speed wireless communication for mobile phones and data terminal: See "LTE (telecommunication)" *Wikipedia* (11 November 2017), online: Wikipedia <https://en.wikipedia.org/wiki/LTE_(telecommunication)>.
3. Dan Goodin, "Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations" *Ars Technica* (28 October 2015), online: Ars Technica <arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/>.
4. *Ibid*.

and private surveillance. As made clear most recently by the revelations of Edward Snowden, private sector organisations are in many ways complicit in surveillance activities by national security organisations. This means that personal data collected within the private sector provides an additional pool of information for law enforcement and national security organisations to utilise.[5]

Modern surveillance practices arguably require a rethinking of some of the tests and assumptions that underlie existing privacy laws, including tests based on "reasonable expectations of privacy", distinctions between content, and between transactional data and content. They also call for active consideration of the full range of regulatory tools available and ways in which they can be adapted to reduce their existing limitations. This paper draws on a range of privacy resources, and on regulatory theory more generally, to suggest possible ways forward.

II. The Problem of Privacy in Public Places

Public place privacy has become a major issue due to technological developments that facilitate "round the clock" surveillance, evolving social practices that increase the amount of information disclosed by individuals about themselves and changes in the decision-making practices of businesses and government agencies involving information obtained via directed, ongoing surveillance as a basis for making decisions about individuals. These are increasingly combining to create what has been described as "seamless, real-time surveillance".[6]

The link between technology and issues of privacy is by no means

5. See *e.g.* Ewen MacAskill & Dominic Rushe "Snowden document reveals key role of companies in NSA data collection" *The Guardian* (1 November 2013), online: The Guardian <www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms>. This threat is arguably amplified to the extent that countries impose compulsory data retention regimes. For useful discussion of the Australian context see Dan Svantesson, "Systematic Government Access to Private-Sector Data in Australia" (2012) 2:4 International Data Privacy Law 268.
6. Edem Williams & Bassey Eyo, "Ubiquitous Computing: The Technology for Boundless Surveillance" (2012) 3:9 International Journal of Scientific & Engineering Research 1 at 2.

new. Early concerns about effects on privacy were highlighted by Warren and Brandeis back in 1890.[7] They related to "instantaneous photographs" and numerous mechanical devices that threatened to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops".[8]

The impact of technology accelerated in the latter part of the 20th century with the advent of digitisation and the convergence that it facilitated, as well as developments such as the increased use of loyalty cards and closed circuit television ("CCTV") cameras.[9] It has accelerated even further in the new millennium due, in particular, to three trends: (1) the proliferation of Radio Frequency Identification ("RFID") that facilitates comprehensive but unobtrusive 'round the clock' surveillance via its use, for example, on freeway transponders and public transport swipe cards; (2) the increased use of Global Positioning Systems ("GPS") to collect data about individuals' geographical locations across time, thereby creating detailed profiles not only of an individual's movements but also of their interrelationships with others; and (3) advances in imaging algorithms (for example, those used for face recognition and automatic number plate recognition), which facilitate the automated operation of CCTV networks and other visual surveillance activities.[10]

These technologies are converging and being combined to create powerful, networked surveillance systems that come close to realising Weiser's vision of a new era of ubiquitous computing ("ubicomp"). This ubicomp era is one in which computer technology would become embedded in all aspects of daily life and computing would increasingly "move to the background, weave itself into the fabric of everyday living

7. Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193.
8. *Ibid* at 195.
9. For a useful overview of these and other early technology-related issues see Australian Law Reform Commission, *Review of Australian Privacy Law* (Discussion Paper No 72) (ALRC 2007) ch 6 (September 2007), online: ALRC <https://www.alrc.gov.au/sites/default/files/pdfs/publications/DP72_full.pdf>.
10. See *e.g.* Christopher Kuner et al, "Face-to-data — Another Developing Privacy Threat?" (2013) 3:1 International Data Privacy Law 1.

spaces and disappear from the foreground, projecting the human user into it".[11] The coupling of RFID technology with internet developments heralds the development of a new "Internet of Things" in which networked controls, sensors and devices for collecting data will increasingly be built into common gadgets, including household appliances, cars and the power grid, permitting "connectivity for anything".[12] The Internet of Things allows further profiling of individuals via the inanimate things with which they are associated by "subjecting more and more previously unobservable activity to electronic measurement, observation, and control".[13] Examples of this development include technologies for monitoring home wearable computing devices,[14] tools used by individuals to track their health and fitness and smart power devices.[15] Moreover, "innovation in this space is already occurring at an extremely rapid pace, thanks to the same underlying drivers of the Internet economy, namely

11. Maja Pantic et al, *Human Computing and Machine Understanding of Human Behavior: A Survey: Proceedings of the 8th International Conference on Multimodal Interfaces, Banff, 2006* (New York: ACM Publications, 2006) 239.
12. Marianna Tafich, "The Internet of Things: Application Domains" in Eckehard Steinbach et el, eds, *Advances in Media Technology: Internet of Things* (Technische Universität München, 2013) at 37 (15 January 2013), online: Advances in Media Technology <citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.395.23&rep=rep1&type=pdf>.
13. Neil M Richards, "The Dangers of Surveillance" (2013) 126:7 Harvard Law Review 1934 at 1940.
14. See Melanie Swan, "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0" (2012) 1:3 Journal of Sensor and Actuator Networks 217.
15. See Joseph Savirimuthu, "Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance" (2013) 27:1–2 International Review of Law, Computers & Technology 161.

Moore's Law[16] and Metcalfe's Law".[17]

Developments that facilitate surveillance have a close interrelationship with decision-making practices. Surveillance technology opens up new possibilities for making use of data, while the increasingly voracious appetite for personal data is fuelling further technological innovation. As noted by Lyon, vast quantities of data are collected, stored and assessed to create profiles and risk categories with an aim toward planning, predicting and preventing "by classifying and assessing those profiles and risks".[18] This allows for more streamlined and better-targeted decision-making, but it also facilitates a level of "social sorting" that is both non-transparent and potentially discriminatory.

While these practices are by no means new, they have been taken a step further via the use of algorithms to mine the vast pools of data that are now available for analysis. As explained by Zarsky, these algorithms are used "to reveal association rules and clusters within the data that might not have been apparent to the analyst initially sifting through the information", producing results that are unpredictable for the analyst and the data subjects and facilitating the revelation of more patterns and

16. As described by Ian Brown, "Computer processing power is expected to continue following Moore's Law, doubling every 18–24 months — at least thirty-fold in the next decade, although by that point the fundamental limits of silicon engineering will be approaching": UK, Government Office for Science, *Future Identities: Changing Identities in the UK: The Next 10 Years – full report*, by Ian Brown, DR 5 (London: Foresight Future Identities, 2013), 1.2.

17. Adam Thierer, "Privacy and Security Implications of the Internet of Things" *Social Science Research Network* (1 June 2013), online: SSRN <www.ssrn.com/abstract=2273031>, at 3, n 20, citing Michael Chui, Markus Löffler & Roger Roberts, "The Internet of Things" *McKinsey Quarterly* (March 2010), online: McKinsey & Company <www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things>.

18. See David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies" in David Lyon, ed, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (London: Routledge, 2003) at 13.

correlations.[19] These techniques are used to mine "Big Data"; that is, "datasets whose size is beyond the ability of typical database software to capture, store, manage, and analyse".[20]

III. Why Loss of Anonymity Requires Attention

Technology-facilitated surveillance is arguably a problem because it undermines the ability of individuals to remain anonymous beyond the narrow confines of private places. This, in turn, makes them potentially vulnerable to a range of harms, ranging from behavioural manipulation through to exploitation, discrimination, identity theft and stalking.

Lack of public place privacy is problematic for reasons similar to those which were identified by privacy advocates when considering the impact of the convergence of computer and telecommunications technologies.[21] These analyses focused on issues of human autonomy and dignity, the use of personal information as a basis for the exercise of power and the lack of dignity inherent in treating individuals as composites of their collated data;[22] they emphasised the important social dimension of anonymity and its role in protecting processes of self-definition and individuation.[23]

Modern observational and information collection activities undermine anonymity by making it difficult, if not impossible, to engage in any publicly observable activities free from identification and surveillance. In doing so they create "a new kind of knowledge …

---

19. Tal Z Zarsky, "*Desperately Seeking Solutions*: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society" (2004) 56:1 Maine Law Review 13 at 27.
20. James Manyika et al, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (McKinsey Global Institute, 2011) at 1.
21. See *e.g.* Moira Paterson, "Privacy Protection in Australia: The Need for an Effective Private Sector Regime" (1988) 26:2 Federal Law Review 371.
22. Austl, Commonwealth, Victorian Law Reform Commission, *Defining Privacy* (Occasional Paper) by Kate Foord (Melbourne: Victorian Law Reform Commission, 2002) at 3.
23. See Jo Ann Oravec, "The Transformation of Privacy and Anonymity: Beyond the Right to be Let Alone" (2003) 39:1 Sociological Imagination 3.

which is re-ordered, codified and made legible to rational, algorithmic understanding"[24] that in turn creates "an ability not only to define 'normal' behavior, but to spot 'abnormal' behaviour through profiling techniques".[25]

Haggerty and Ericson's concept of the "surveillant assemblage"[26] provides a useful device for understanding the nature of the surveillance practices that have arisen in response to the surveillance potential of new technologies. This complex system arises due to the converging interests of multiple public and private bodies in establishing credentials (for example, identity and other personal attributes) and surveillance systems to provide for ways to differentiate amongst unknown strangers. This system is designed to improve the efficiency of decision-making, but it is problematic to the extent that "[l]ack of public anonymity promotes conformity and an oppressive society",[27] and it encourages blandness and conformity, leading to "a blunting and blurring of rough edges and sharp lines".[28]

An alternative metaphor, suggested by Solove, is Kafka's *The Trial*, which highlights the issue of lack of control over information in a context where bureaucratic decisions are increasingly based on dehumanised information processing.[29] This metaphor is useful in emphasising that surveillance can be dangerous and oppressive, even where the intentions that underlie it are inherently benign. The danger lies in the use of surveillance as a basis for automated decision-making and the

---

24. David J Phillips, "Beyond Privacy: Confronting Locational Surveillance in Wireless Communication" (2003) 8:1 Communications Law & Policy 1 at 18.
25. *Ibid*.
26. Kevin D Haggerty & Richard V Ericson, "The Surveillance Assemblage" (2000) 51:4 British Journal of Sociology 605.
27. Christopher Slobogin, "Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity" (2002) 72:1 Mississippi Law Journal 213 at 240.
28. Julie Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52:5 Stanford Law Review 1373 at 1426.
29. Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 36–39.

oppressiveness that this can create in contexts where the individual is unaware of what is being collected and of the potential consequences that might follow.

The end result is what Cohen describes as a process of modulation: "a set of processes in which the quality and content of surveillant attention is continually modified according to the subject's own behavior, sometimes in response to inputs from the subject but according to logics that ultimately are outside the subject's control".[30] As she explains, the very ordinariness of this process makes it extremely powerful, producing citizens who are very different from those which form the basis for the traditional liberal democratic tradition; lack of privacy deprives them of the breathing space to engage in socially situated processes of boundary management, thereby ensuring that "the development of subjectivity and the development of communal values do not proceed in lockstep".[31] This process is not only harmful to individual autonomy but also at odds with broader public policy goals relating to liberal democratic citizenship and innovation.

IV. Existing Regulatory Frameworks and Their Shortcomings

The key regulatory frameworks that are currently used to regulate aspects of surveillance fall into four broad groups; (1) laws that regulate interception of communications; (2) laws that regulate the uses of specific surveillance devices, including listening devices; (3) data protection and other laws that require compliance with fair information handling principles; and (4) common law and statutory rights to sue in the courts.

These frameworks all suffer from a similar shortcoming to that observed by Solove in relation to the United States laws that regulate electronic surveillance: "[t]he degree of protection against certain forms

30. Julie Cohen, "What Privacy is For" (2013) 126:7 Harvard Law Review 1904 at 1915 [Cohen, "What Privacy is For"].

31. *Ibid* at 1911, citing Julie Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012) at 150.

of surveillance often does not turn on how problematic or invasive it is, but on the technicalities of how the surveillance fits into the law's structure".[32]

A. Telecommunications Interception Laws

Surveillance involving the interception of telecommunications (including the accessing of communications stored within telecommunications systems) is generally regulated by telecommunications interception laws. These typically permit law enforcement and national security bodies to intercept telecommunications in specific circumstances, while making interception otherwise illegal.

In Australia, the *Telecommunications (Interception and Access) Act* prohibits: intercepting a "real-time" communication passing over the telecommunications system;[33] accessing an electronic communication such as an email, Small Message Service or voicemail message while it is stored on a telecommunications carrier's (including an Internet Service Provider's) equipment;[34] and communicating or otherwise dealing with illegally intercepted information.[35] These offences carry substantial criminal sanctions. The term "interception" is defined as listening to or recording a conversation by any means without the knowledge of the person making the communication.[36]

---

32. Daniel J Solove, "Reconstructing Electronic Surveillance Law" (2003) 72:6 The George Washington Law Review 1264 at 1298.
33. *Telecommunications (Interception and Access) Act 1979* (Cth) (Austl), ss 7(1), 105.
34. This prohibition applies in circumstances where that message cannot be accessed on that equipment by a person who is not a party to the communication, without the assistance of an employee of the carrier: *Ibid*, ss 5(1) ("stored communication"), 108.
35. *Ibid*, ss 63, 108(1).
36. *Ibid*, s 6(1) ("interception").

The equivalent federal legislation in the United States[37] makes it a federal crime for any person to intentionally intercept (or endeavour to intercept) wire, oral or electronic communications by using an electronic, mechanical or other device,[38] or to intentionally access without authorisation (or to exceed an authorisation to access) a facility through which an electronic communication service is provided and thereby obtain, alter, or prevent authorised access to a wire or electronic communication while it is in electronic storage in such a facility.[39] The term "interception" is defined as the "aural or other acquisition" of the contents of various kinds of communications by means of "electronic, mechanical or other devices",[40] and the prohibition applies both to "electronic communications", which encompass most radio and data transmissions and any communication from a tracking device,[41] and "oral communications", which include any face-to-face conversations for which the speakers have a justifiable expectation of privacy.[42]

In the case of Canada, the *Criminal Code* makes it an offence for

37. These are supplemented by state wiretap laws that are mostly directed at telephone conversations. For example, it is illegal in California to record or eavesdrop on any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation: *California Penal Code*, PEN § 632 (2017) (US); The Citizen Media Law Project provides some selected summaries of state recording laws: The Citizen Media Law Project, "State Law: Recording" *Digital Media Law Project* (2 March 2008), online: Berkman Center for Internet & Society <www.citmedialaw.org/legal-guide/state-law-recording>; there is also a full list of state wiretap laws on the website of the National Conference for State Legislatures at: "Electronic Surveillance Laws" *National Conference of State Legislatures* (23 March 2012), online: NCSL <www.ncsl.org/programs/lis/ CIP/surveillance.htm> [*Electronic Surveillance Laws*].
38. *Electronic Communications Privacy Act*, 18 USC § 2511(1) (2006).
39. *Stored Communications Act 1986*, 18 USC § 2701(a) (2006).
40. *Ibid*, § 2510(4).
41. "Tracking Device" is defined in *ibid*, § 3117(b) as "an electronic or mechanical device which permits the tracking of the movement of a person or object'".
42. *Ibid*, § 2510(2). The meaning of "oral communications" is discussed in *United States v Larios*, 593 F Supp (3d) 82 at 92 (1st Cir 2010) (US).

anyone to "by means of any electro-magnetic, acoustic, mechanical or other device wilfully [intercept] a private communication".[43] The term "private communication" is defined broadly to include any oral communication or telecommunication, including "any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it".[44] Interception includes listening to, recording or acquiring a communication, or acquiring its substance, meaning or purport.[45]

Interception laws provide valuable protection for communications that take place over telecommunications systems, but they commonly suffer from two key defects. The first is that, in countries such as Australia and the United States, they protect only communications that involve the use of telecommunications systems, as opposed to, say, oral communications or communications via Bluetooth technology. They also typically offer differential protection based on artificial distinctions between transactional and content data, with the former receiving a much lower level of, or no, protection based on the increasingly incorrect assumption that transactional data is inherently less privacy invasive than communicative content.[46]

However, the nature and extent of metadata that can now be collected means that it can be as, or even more, revealing than content data. As noted by a former Ontario Information and Privacy Commissioner:

> Access to [metadata] will reveal the details of our personal, political, social, financial, and working lives. It provides the raw material for the creation of detailed, comprehensive, time-stamped map-lines of who is communicating with whom, when, how often, and for how long; where the senders and recipients are located; who else is connected to whom, and so forth.[47]

Research conducted at Stanford illustrates the potentially revealing nature

43. *Criminal Code*, RSC 1985, c C-46, s 184(1).
44. *Ibid*, s 183.
45. *Ibid*.
46. *Ibid*.
47. Office of the Ontario Privacy Commissioner, "A Primer on Metadata: Separating Fact from Fiction", by Ann Cavoukian, PhD, Information and Privacy Commissioner (Ontario: IPC, July 2013) at 12.

of metadata. The study involved 546 participants who ran an application on their cell phones that submitted device logs and social network information for analysis.[48] In analysing their results, the researchers commented that the degree of sensitivity relating to persons and organisations contacted by the participants had taken them aback. The persons contacted included "Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more".[49] The researchers also discussed potential inferences that could be made from patterns of calls and referred to a number of examples, including a participant who had communicated with "multiple local neurology groups, a specialty pharmacy, a rare condition management service and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis"[50] and another who in the space of three weeks "contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop".[51]

B. Surveillance Device Laws: Listening Devices and Beyond

Surveillance devices laws offer protection against specific uses of surveillance devices. They generally regulate uses of listening devices but may also extend more broadly to other categories of devices, including those used to track the location of individuals and items with which they are associated (such as cars) and optical surveillance devices, including CCTV cameras.

---

48. "What's in Your Metadata?" *The Center for Internet and Society* (2013), online: Stanford Law School <https://cyberlaw.stanford.edu/blog/2013/11/what%27s-in-your-metadata>.
49. Jonathan Mayer & Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata" *Web Policy* (blog) (12 March 2014), online: Web Policy <www.webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>.
50. *Ibid*.
51. *Ibid*. "Head shop" is a colloquial expression used to describe an enterprise that retails items used for the consumption of cannabis or related to the cannabis culture.

In the case of the United States, surveillance device regulation is not the norm, and listening is regulated primarily via interception laws, as discussed above, although a small number of states impose restrictions on visual surveillance.[52] For example, the *Georgia Penal Code* makes it an offence to "to observe, photograph, or record the activities of another which occur in any private place and out of public view".[53]

In contrast, surveillance device laws are commonplace at the state and territory levels in Australia.[54] For example, the Victorian *Surveillance Devices Act* contains general prohibitions against the use of listening devices, optical surveillance devices and tracking devices.[55] As in the case of telecommunications interception, these are subject to exceptions in respect of authorised activities of law enforcement and national security bodies. These are also subject to a number of restrictions that limit their operation in public places. For example, the listening device prohibition is limited by reference to a test based on reasonable expectation of being overheard,[56] the optical surveillance prohibition is limited in its application to surveillance of indoor activities and by reference to a test based on reasonable expectation of being seen[57] and the definition of

52. The website of the National Conference for State Legislatures at *Electronic Surveillance Laws*, *supra* note 37, contains details of state laws which impose restrictions on visual surveillance.
53. 11 Ga Code Ann tit 16 § 16-11-62 (2010) (US). This prohibition is subject to a number of exceptions set out in paras (A)–(C).
54. *Listening Devices Act 1992* (ACT) (Austl); *Surveillance Devices Act 2007* (NSW) (Austl); *Surveillance Devices Act* (NT) (Austl); *Invasion of Privacy Act 1971* (Qld) (Austl); *Listening and Surveillance Devices Act 2016* (SA) (Austl); *Listening Devices Act 1991* (Tas) (Austl); *Surveillance Devices Act 1999* (Vic) (Austl); and *Surveillance Devices Act 1998* (WA) (Austl).
55. *Surveillance Devices Act 1999* (Vic) (Austl), ss 6–8. Section 9 also contains a prohibition against the use of "data surveillance devices" (see definition in s 3(1)) but this is limited in its application to law enforcement officers. The prohibitions in these sections related to the installation, use and maintenance of surveillance devices and are supplemented by further prohibitions in ss 11 and 12 against the communication and publication of data wrongfully obtained via use of surveillance devices.
56. *Ibid*, ss 3(1) (definition of "private conversation"), 6(1).
57. *Ibid*, ss 3(1) (definition of "private activity"), 7(1).

tracking device is limited to devices designed solely for tracking[58] (so does not therefore apply, for example, to cell phones).

These tests are based on assumptions that are arguably no longer appropriate due to technological developments. For example, the fact that one might reasonably expect to be seen by a random passer-by does not mean that one should expect to be photographed by a distant camera equipped with face recognition technology. As observed by Boa in relation to common law tests based on reasonable expectations of privacy, "[t]echnological capabilities and the resulting information practices are constantly changing. As a result, social norms of what is reasonable have not been, and arguably cannot be, established".[59]

In the case of Canada, specific regulation of surveillance devices is likewise not the norm and listening is regulated primarily via the prohibition against interception discussed above. In addition, various uses of surveillance devices, including optical surveillance devices[60] and the use of GPS tracking devices,[61] have been held to qualify as searches, although their reasonableness will depend on the specific context.

Surveillance device laws have the advantage of being tied specifically to the devices used for surveillance but, even to the extent that they are comprehensive in terms of the types of devices covered, these laws generally offer minimal protection against surveillance in public places due to the inherent problems in finding tests that capture what matters without encroaching unduly on other competing interests. They may also be of limited assistance to the extent that they fail to encompass the full spectrum of devices that may potentially be used for the purposes of surveillance.

This issue arises most acutely in relation to optical surveillance devices due to the need to ensure that they do not impact adversely

---

58. *Ibid*, ss 3(1) (definition of "tracking device"), 8(1).
59. Kristin Boa, "Privacy Outside the Castle: Surveillance Technologies and Reasonable Expectations of Privacy in Canadian Judicial Reasoning" in David Matheson, ed, *Contours of Privacy* (Newcastle: Cambridge Scholars, 2009) 241 at 244.
60. *R v Wong*, [1990] 3 SCR 36 at para 61.
61. *R v Wise*, [1992] 1 SCR 527.

on legitimate uses of cameras. Abandonment of tests based on indoor/outdoor distinctions and reasonable expectations of being seen, raises the issue of how to distinguish between activities that are legitimate (for example, taking a photograph for personal or artistic purposes) and those that should be prohibited (for example, surreptitious filming of activities that are clearly private in nature such as long lens filming of a couple making love in a location that is secluded but outdoors).

C. Common Law and Statutory Rights of Action for Breaches of Privacy

Common law and statutory rights of action fall into two main groups. The first comprises common law rights of action based on some or all of the four United States privacy torts set out in the *Restatement (Second) of Torts*;[62] these also form the basis for most statutory rights of action in Canada.[63] The second is the extended action for breach of confidence, which has been developed by courts in the United Kingdom[64] and is

62. *Restatement (Second) of Torts* (Washington DC: American Law Institute, 1977) at §§ 657B-E [American Law Institute]; intrusion upon seclusion, appropriation of name or likeness, publicity given to private life and publicity placing person in false light.

63. For example, the Canadian provinces of British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador all have statutory privacy torts: see *Privacy Act*, RSBC 1996, c 373; *The Privacy Act*, RSS 1978, c P-24; *The Privacy Act*, RSM 1987, c P-125; *An Act Respecting the Protection of Personal Privacy*, RSNL 1990, c P-22; together referred to as ["Canadian Provincial Statutory Privacy Torts"].

64. For example, this is seen in the leading cases of *Campbell v MGN Ltd,* [2004] UKHL 22 [*Campbell*], and *Mosley v News Group Newspapers Ltd,* [2008] EWHC 1777 (QB).

currently under active consideration in Australia.[65]

In the case of the former, the intrusion tort is more obviously directed to the regulation of surveillance, as it focuses on the invasion of the private sphere (rather than on the publication of personal data)[66] and has been interpreted as being capable of extending to surveillance conducted in public places.[67] However, while it creates less obvious First Amendment issues than the public disclosure tort, it has nevertheless been construed, at least in some cases, as being subject to newsworthiness privilege.[68] The intrusion tort has been recognised recently in Canada[69] and New Zealand,[70] although it remains unclear to what extent it will be recognised as applying to public place surveillance. There are also a number of jurisdictions that have statutory intrusion torts.[71]

The other privacy tort that may be indirectly relevant is the public disclosure tort, which regulates the public disclosure of private facts, including those acquired via surveillance. However, this is generally of

65. In *Australian Broadcasting Corporation v Lenah Game Meats*, [2001] HCA 63, Gleeson CJ supported an extension of the action of breach of confidence to protect private information. While that court has yet awarded relief on this basis, the decision of the Victorian Court of Appeal in *Giller v Procopets*, [2008] VSCA 236 (Austl), has arguably further paved the way for such a development by following English case law in deciding that damages for breach of confidence can be awarded for mental distress falling short of psychiatric injury.
66. See Adam J Tutaj, "Intrusion Upon Seclusion: Bringing an 'Otherwise' Valid Cause of Action into the 21st Century" (1999) 82:3 Marquette Law Review 665.
67. See *e.g. Wolfson v Lewis*, 924 F Supp 1413 at 1433–35 (Dist Ct Pa 1996) (US). See further, Carmin L Crisci, "All the World is Not a Stage: Finding a Right to Privacy in Existing and Proposed Legislation" (2002) 6:1 New York University Journal of Legislation & Public Policy 207 at 228–30.
68. See *Dempsey v National Enquirer*, 702 F Supp 927 at 930–31 (Dist Ct Me 1988) (US). For further examples see Lyrissa B Lidsky, "Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It" (1999) 73:1 Tulane Law Review 173 at 209, n 187.
69. *Jones v Tsige,* 2012 ONCA 32.
70. *C v Holland,* [2012] NZHC 2155.
71. See *e.g.* Canadian Provincial Statutory Privacy Torts, *supra* note 63; American Law Institute, *supra* note 62.

limited assistance in relation to public place surveillance as it runs directly into conflict with freedom of expression/speech. This is a major problem in the United States due to the strength of First Amendment protection but is also an issue in New Zealand, which recognises a similar tort.[72]

It is also problematic to the extent that it contains an offensiveness test that relates to the information disseminated, as opposed to the method by which it was obtained, and ignores the dignitary harm resulting from the surveillance activities that underpin the disclosure. This issue has attracted discussion in New Zealand in the aftermath of the decision in *Andrews v Television New Zealand*[73] in which the court declined to award relief in respect of the broadcast of footage of the plaintiffs being extracted from the wreckage of their car, even though the court found that they had a reasonable expectation of privacy in relation to their conversations with each other.[74]

The extended action for breach of confidence demonstrably provides better protection for privacy in public places.[75] However, as currently formulated, it requires the disclosure of personal information and is therefore not inherently suited to the regulation of surveillance *per se*. Moreover, it does not regulate surveillance, however intrusive on privacy, if the information acquired is not disclosed to other persons.

More generally, it is arguable that privacy-based rights of action have the advantage of focussing squarely on the interest that is in issue, but they create difficulty because of the nebulous nature of privacy as a concept and the fact that it generally rubs up against other competing rights. The

---

72. See Moira Paterson, "Criminal Records, Spent Convictions and Privacy: A Trans-Tasman Comparison" (2011) 69:1 New Zealand Law Review 69 at 74–76.
73. *Andrews v Television New Zealand*, [2009] 1 NZLR 220 (HC).
74. For a useful critique on the New Zealand tort see Nicole A Moreham, "Why is Privacy Important? Privacy, Dignity and Development of New Zealand Breach of Privacy Tort" in Jeremy Finn & Stephen Todd, eds, *Law, Liberty, Legislation: Essays in Honour of John Burrows, QC* (Wellington: LexisNexis, 2008), online: Victoria University of Wellington <www.victoria.ac.nz/law/pdf/nm-law-liberty-legislation.pdf>.
75. This is evident from the outcomes in *Campbell, supra* note 64, and *Murray v Big Pictures (UK) Ltd*, [2008] EWCA Civ 446.

problem, therefore, lies in devising a test that is sufficiently certain and at the same time strikes an appropriate balance between privacy and other competing rights, such as freedom of expression/speech.

D. Data Protection Laws and Other Laws Based on Fair Information Practices ("FIPs")

Data protection laws protect privacy by requiring compliance with FIP-based rules that regulate the handling of personal information. They are relevant to surveillance insofar as they impose limitations on the collection (and subsequent use of) personal information. Instead of being based on the type of device or communication system being used to collect data, they focus on the nature of the data in question and whether or not it relates to an individual who is identified or potentially identifiable. Schwartz & Solove refer to this concept as "personally identifiable information".[76]

The concept of regulation via fair information principles has its origins in the United States in a report by the Advisory Committee on Automated Personal Data Systems in the Department of Health, Education and Welfare.[77] These principles formed the basis for the public sector regime in the *Privacy Act* in the United States[78] and also for the

76. Paul M Schwartz & Daniel J Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Data" (2011) 86:6 New York University Law Review 1814.

77. US, Department of Health, Education and Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computes and the Rights of Citizens* (No (OS) 73-94) (Washington DC: DHEW Publication, 1973).

78. 5 USC § 552a (1974) [US *Privacy Act*].

Safe Harbor principles[79] administered by the Federal Trade Commission, as well as for the many data protection regimes that exist throughout the world.[80]

The United States is unusual in terms of its lack of any FIP-based regime of general application to the private sector, although the FIPs form the basis for many federal and state laws[81] and are summarised in set of principles developed by the FTC to provide guidance concerning privacy-friendly, consumer-oriented data collection practices.[82]

The federal public sector *Privacy Act*[83] regulates information handling by federal agencies via a Code of Fair Information Practice.[84] It requires inter alia that agencies must "collect information to the greatest extent practicable directly from the subject individual when the information

---

79. Full details about this regime can be accessed online: US, Federal Trade Commission, "U.S.-E.U Safe Harbor Framework" (FTC, 25 July 2016), online: FTC <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework>. It should be noted that the Safe Harbor Framework is no longer legally recognised as adequate under EU law for transferring personal data to the US and that the US and EU have now negotiated a new Privacy Shield Network, see "Privacy Shield Framework" *International Trade Administration*, online: ITA <https://www.privacyshield.gov/welcome>. The latter contains further additional protections.
80. For a useful overview of the evolution of laws based on FIPs see Fred Cate, "The Failure of Fair Information Practice Principles" in Jane K Winn, ed, *Consumer Protection in the Age of the 'Information Economy'* (Abingdon: Taylor and Francis, 2006) 341 [Cate, "Fair Information Practice Principles"].
81. See *e.g. The Fair Credit Reporting Act,* 15 USC § 1681 (1970); *Right to Financial Privacy Act,* 12 USC § 3401 (1978); *Electronic Communications Privacy Act* of 18 USC §§ 2510-252 (1986). For a useful overview of a number of FIP-based laws in the US, see Schwartz & Solove, *supra* note 76.
82. US, Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998) at 7–14.
83. US *Privacy Act*, *supra* note 78.
84. US, Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Data Systems, Records, Computers, and the Rights of Citizens, *Code of Fair Information Practice* (HEW, July 1973).

may result in adverse determinations about an individual's rights, benefits, and privileges under any Federal program".[85] It also prohibits the maintenance of any record "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity".[86]

The *Privacy Act* generally applies only to systems of records — i.e. "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual".[87] The term "record" is defined as:

> [A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.[88]

In *Albright v United States*[89] the court held that a videotape of a meeting qualified as record as it contained a means of identifying an individual by picture or voice and that it contravened the *Act* by showing an individual exercising their First Amendment rights (by making complaints about their employment).[90] The court also held that it did not matter in that case that the videotape was not maintained in a system of records, as this specific prohibition applied to agencies more generally.

In Australia, the *Privacy Act*[91] was once similarly confined to the

85. US *Privacy Act*, *supra* note 78**,** § 552a(e)(2).
86. *Ibid***,** § 552a(e)(7).
87. *Ibid***,** § 552a(a)(5).
88. *Ibid*, § 552a(a)(4).
89. 631 F (2d) 915 at 920 (DC Cir 1980) (US).
90. This case is discussed in Robert Gellman, "A General Survey of Video Surveillance Law in the United States" in Sjaak Nout, Berend de Vries & Corien Prins, eds, *Reasonable Expectation of Privacy?: Eleven Country Reports on Camera Surveillance and Workplace Privacy* (The Hague: TMC Asser Press, 2005) 7.
91. *Privacy Act 1988* (Cth) (Austl) [Austl *Privacy Act*].

public sector, but it now applies also to the private sector and has recently been amended to include a single set of *Australian Privacy Principles* ("*APPs*") that apply to information handling by both sectors.[92] The application of the *APPs* to the private sector is, however, subject to a large number of exceptions, including exceptions for the journalistic practices of media organisations[93] and for acts of individuals acting in a non-business capacity.[94]

The *APPs* govern the handling of "personal information", which is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable.[95] This is a new definition[96] that has been designed to require "a consideration of the cost, difficulty, practicality and likelihood that the information will be linked in such a way as to identify [the individual]".[97] This has the effect that the records of surveillance are not covered by the *Act* unless they contain images or other data that allow for recognition of the individuals to which

92. The *Privacy Act* is supplemented by laws that operate in a similar way in relation to most government agencies in most states and the Northern Territory: *Privacy and Personal Information Protection Act 1998* (NSW) (Austl); *Information Act 2000* (NT) (Austl); *Information Privacy Act 2009* (Qld) (Austl); *Personal Information Protection Act 2004* (Tas) (Austl); *Privacy and Data Protection Act 2014* (Vic) (Austl). There is a detailed overview of the Privacy Act in Moira Paterson, "Privacy" in Matthew Groves, ed, *Modern Administrative Law in Australia: Concepts and Context* (Port Melbourne: Cambridge University Press, 2014).
93. Austl *Privacy Act*, *supra* note 91, s 7B(4).
94. *Ibid*, s 7B(1).
95. *Ibid*, s 6(1).
96. It was amended by the *Privacy Amendment (Enhancing Privacy Reform) Act 2012* (Cth) (Austl).
97. Austl, Commonwealth, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108) (ALRC, 2008) at 6.57. This approach is consistent with that taken by the Victorian Civil and Administrative Tribunal in interpreting a similar (but not identical) provision in the *Information Privacy Act 2000* (Vic) (Austl): See *WL v La Trobe University*, [2005] VCAT 2592 (Austl). For a further discussion of the Australian provisions, see Mark Burdon & Paul Telford, "The Conceptual Basis of Personal Information in Australian Privacy Law" (2010) 17:1 Murdoch University, Electronic Journal of Law 1.

they relate, or unless they have been collected in a context in which the collecting organisation can readily link them to other data that identifies an individual.

This issue has arisen for consideration in recent litigation concerning an application made under the *Privacy Act* for access to the applicant's mobile network data. In *Telstra Corporation Ltd v Privacy Commissioner*, the Commonwealth Administrative Appeals Tribunal found against the applicant on the ground that this data did not constitute "personal information".[98] In the tribunal's view, the metadata in question was "all about the way in which Telstra delivers the call or the message. That is not about Mr Grubb".[99] This decision was upheld by the Full Court of the Federal Court of Australia, which expressed the view that the words "about an individual" in the definition of personal information raised a threshold question that needed to be addressed before it could be determined whether that individual is identified or identifiable.[100] In the court's view, it was necessary in every case to consider whether each item of personal information requested, individually or in combination with other items, was "about an individual". This would "require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity [could] reasonably be ascertained will require an evaluative conclusion".[101]

The *APPs* include a collection limitation principle, which requires that personal information be collected fairly and legally[102] and precludes the collection of personal information unless it is reasonably necessary for one or more of the functions or activities of the organisation collecting it.[103] They also include further principles relating to open and transparent

98. [2015] AATA 991.
99. *Ibid* at para 112.
100. *Privacy Commissioner v Telstra Corporation Ltd*, [2017] FCA 4 at para 89.
101. *Ibid* at para 63; See also Normann Witzleb, "'Person Information' under the Privacy Act 1988 (Cth) – Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4" (2017) 45:2 Australian Business Law Review 188.
102. *Australian Privacy Principles, APP* 3.5, being Schedule 1 of the *Privacy Act 1988* (Cth) (Austl).
103. *Ibid*, *APP* 3.2.

management,[104] notification of the collection of personal information,[105] limitations on use and disclosure,[106] requirements to maintain security[107] and integrity[108] and obligations to provide access to information subjects.[109]

Oversight of the *Privacy Act* is provided by the Office of the Australian Information Commission. The Commissioner's functions are grouped within the Act according to whether they foster compliance (via the provision of guidance),[110] monitor compliance[111] or support compliance (via the provision of advice).[112] The Act is enforced primarily via a complaints-based system, although the Information Commissioner also has power to conduct audits to assess entities' maintenance of personal information,[113] to require provision of privacy impact assessments[114] and to conduct "own motion" investigations.[115]

Canada differs in that it has separate federal privacy regimes. The *Privacy Act*[116] and the *Personal Information Protection and Electronic Documents Act*[117] govern the information handling practices of the federal government and private organisations, respectively. These both require compliance with sets of FIPs that apply in respect of "personal information". The latter is defined as "information about an identifiable

104. *Ibid, APP* 1.
105. *Ibid*, *APP* 5.
106. *Ibid*, *APP* 6.
107. *Ibid*, *APP* 10.
108. *Ibid*, *APP* 11.
109. *Ibid*, *APP* 12.
110. *Ibid*, s 28.
111. *Ibid*, s 28A.
112. *Ibid*, s 28B.
113. *Ibid*, s 33C.
114. *Ibid*, s 33D(1); A "privacy impact assessment" means a written assessment that identifies the impact an activity or function might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact: Also see *ibid*, s 33D(3).
115. *Ibid*, s 40.
116. *Privacy Act*, RSC 1985, c P-21 [Canada *Privacy Act*].
117. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

individual".[118] Both Acts are subject to oversight by the Office of the Privacy Commissioner of Canada.

A problem with laws based on FIPs is that they depend on the criterion of personally identifiable information ("PII") to establish their boundaries. As explained by Schwartz and Solove, without these boundaries "privacy rights would expand to protect a nearly infinite array of information, including practically every piece of statistical or demographic data".[119] However, the criterion of identifiability is inherently fluid and whether or not information is reasonably identifiable depends on how much effort is put into the process, to what extent linkage with other available information is relevant and the extent to which it is appropriate to consider new and emerging identification technologies. Furthermore, determining where precisely to set the boundaries for identifiability raises difficult policy issues given that information that qualifies as personal information is generally subject to the full spectrum of requirements set out in the legislation.

Take, for example, a CCTV image of someone who is not immediately identifiable but who may be identified if face recognition technology is applied to the footage. From a privacy perspective, collection *per se* is of minimal privacy invasiveness if the footage is simply kept for a period to determine if it is required, say, to assist in the detection of pilfering, and then disposed of without that individual ever having been identified. However, if that image qualifies as personal information based on the fact that the individual could be identified, the collector would be required to provide access to it on request — a requirement which might be quite onerous depending on the ease of location of the image required and the need to protect the identities of any other persons who feature in the same footage (assuming that their images also qualify as personal information). On the other hand, if it does not qualify as personal information, the collector will not be under any obligation to keep the footage secure and would not be precluded from disclosing it to another individual who may have some means of recognising the individual.

---

118. Canada *Privacy Act*, *supra* note 116, s 3; *PIPEDA*, *ibid*, s 2(1).
119. Schwartz & Solove, *supra* note 76 at 1866.

A test based on identifiability also creates problems for the reasons suggested by Ohm — *i.e.* that the science of reidentifiability increasingly undermines processes of anonymization by deleting from information personal identifiers such as names and context specific identifiers such as identity numbers, account numbers, etc.[120] Millard and Hon have likewise commented that "scientific and technological advances are making it increasingly simple to de-anonymise data to 're-identify' individuals, notwithstanding the use of methods such as aggregation or barnardisation"[121] and that this may mean that "almost all data could qualify as 'personal data', thereby rendering PII meaningless as a trigger for data protection obligations".[122]

Another issue identified by Cate is that the effectiveness of current FIP-based laws depends on a control-based system that relies on procedures designed to maximise individual control, for example, via requirements for notice and consent.[123] However, consent has become an increasingly artificial construct given the complexity of the "surveillant assemblage" and the fact that individuals have little prospect of understanding the significance of individual data disclosures. Furthermore, "[n]otices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice".[124]

---

120. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57:6 UCLA Law Review 1701.
121. Barnardisation is "[a] method of disclosure control for tables of counts that involves randomly adding or subtracting 1 from some cells in the table": See online: "Glossary of Statistical Terms" *Organisation for Economic Co-operation and Development* (9 November 2005), online: OECD <stats.oecd.org/glossary/detail. asp?ID=6887>.
122. Christopher Millard & W Kuan Hon, "Defining 'Personal Data' in E-Social Science" (2011) 15:1 Information, Communication & Society 66 at 77.
123. Cate, "Fair Information Practice Principles", *supra* note 80 at 341.
124. *Ibid* at 3.

V. The Significance of Constitutional/Human Rights Frameworks

A difficulty in providing effective regulation of public place surveillance is that laws that provide strong privacy protections may be viewed as undermining the freedom of the press/freedom of speech to the extent that they restrict the surveillance that facilitates the dissemination of personal information about individuals.

Constitutional frameworks play an important role in determining the nature and extent of the privacy regulation that is possible. This is most evident in the United States, where the strength of the First Amendment protection of free speech and the lack of equivalent protection of informational privacy beyond the specific context of search and seizure creates major difficulties. It is also the case in other countries, such as Canada[125] and New Zealand,[126] which have human rights laws that lack express privacy guarantees. The European Human Rights regime, which provides specific protection for privacy, as well as for freedom of expression, provides greater flexibility.[127]

However, it is arguable that the interests served by effective regulation of surveillance are in many cases identical to those which underlie the important right to free speech. As identified many years ago by Regan, privacy has suffered due to its conception as an individual right, which

125. The *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (UK), 1892, c 11, contains a right to "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication" (s 2(b)) and a right "to be secure against unreasonable search or seizure (s 8), but no general right to privacy".

126. The *New Zealand Bill of Rights Act 1990* (NZ), 1990/109 contains a right to "freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form" (s 14) and a right to be "secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise" (s 21), but not any right to privacy more generally.

127. *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 at 223 arts 8–10 (entered into force 3 September 1953).

means that it fares badly when it conflicts with competing rights that are traditionally conceived of as serving broader public purposes.[128]

The individualistic view of privacy is frequently articulated in the language of a negative freedom (*i.e.* as a freedom from interference by other people)[129] and one that is in essence "anti-social" and pertaining to the "right of an individual to live a life of seclusion and anonymity, free from the prying curiosity which accompanies both fame and notoriety".[130] However, privacy may equally be conceived of as a positive claim to a status of personal dignity, premised on the ability to exercise some element of control over one's own personal information. In that sense it is not "simply an absence of information about us in the minds of others. Rather, it is the control we have over information about ourselves".[131]

Moreover, while there can be no doubt that a right to privacy is an integral feature of liberal democratic systems that value individual autonomy and dignity (in particular, the right to be treated as a human being and not some abstract object), privacy also serves broader societal goals. As explained by Raab, in the context of surveillance, lack of privacy disrupts communication, resulting in an isolation that is inconsistent with democracy;[132] "participatory freedoms require a degree of privacy" (as illustrated by the nexus between free elections and secret ballots).[133]

It follows, therefore, that it is erroneous to conceive of anti-surveillance laws as necessarily contravening free speech protection or overstepping a permissible balance between privacy and freedom of expression. That is

---

128. Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (North Carolina: University of North Carolina Press, 1995).
129. See Isaiah Berlin, "Two Concepts of Liberty" in Isaiah Berlin, ed, *Four Essays on Liberty* (Oxford: Oxford University Press, 1969) 15, online: University of Hamburg <www.wiso.unihamburg.de/fileadmin/wiso_vwl/johannes/Ankuendigungen/Berlin_twoconceptsofliberty.pdf>.
130. Louis Nizer, "The Right of Privacy: A Half Century's Developments" (1941) 39:4 Michigan Law Review 526 at 528.
131. Charles Fried, "Privacy" (1968) 77:3 Yale Law Journal 475 at 482.
132. Charles Raab, "Privacy, Democracy, Information" in Brian Loader, ed, *The Governance of Cyberspace: Politics, Technology and Global Restructuring* (London: Routledge, 1997) 153 at 157.
133. *Ibid* at 160.

not to suggest that there is not potential conflict between the two, rather that it is important to bear in mind that failure to prevent the process of modulation described by Cohen in many respects renders meaningless the protection of the right to speech.

VI. Insights From Regulatory Theory

The theory of responsive regulation developed by Ayers and Braithwaite contends that:

> the achievement of regulatory objectives is more likely when agencies display both a hierarchy of sanctions and a hierarchy of regulatory strategies of varying degrees of interventionism. ... Regulators will do best by indicating a willingness to escalate intervention up those pyramids or to deregulate down the pyramids in response to the industry's performance in securing regulatory objectives.[134]

This is further explained on the basis that "[t]he pyramidal presumption of persuasion gives the cheaper, more respectful option a chance to work first. More costly punitive attempts at control are thus held in reserve for the minority of cases where persuasion fails".[135] The regulatory pyramid[136] therefore has softer measures such as warnings, persuasion and collaboration at its base, followed by civil sanctions and then criminal sanctions at its apex.

Telecommunications interception and surveillance device laws generally rely on the impositions of criminal sanctions. These have a strong deterrent effect but require a high standard of proof for convictions and rely on police for their enforcement**.** This is not necessarily conducive to good outcomes, as illustrated by the Murdoch media scandal in the United Kingdom. The regulatory pyramid suggests that criminal sanctions should be used only as a last resort in respect of more egregious conduct and that they are inherently unsuitable as a sole or primary device for achieving across-the-board regulatory outcomes in

134. Ian Ayers & John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992) at 5–6.
135. John Braithwaite, "Responsive Regulation and Developing Economies" (2006) 34:5 World Development 884 at 887.
136. Ayers & Braithwaite, *supra* note 134 at 39.

the surveillance context.

Common law and statutory torts focus instead on providing appropriate remedies for individuals who are adversely affected by non-compliance. However, they produce a deterrent effect only to the extent that individuals are able to identify those responsible for privacy breaches that have caused (or are likely to cause) them harm and are then willing to litigate, bearing in mind that litigation may of itself be harmful to their privacy. Also they are likely to have a deterrent effect only if the damages available are sufficiently large to outweigh the potential profits to be gained from non-compliance. Furthermore, the fact these torts are available only to provide redress in respect of the types of harm that are capable of attracting legal compensation means that they are not well suited to addressing the harms inherent in the processes of modulation. It is arguable, therefore, that this purely private focus limits their usefulness as a sole or primary device for regulating surveillance.

On the other hand, data protection regimes provide for a more flexible range of regulatory options, including ones at the softer end of the spectrum (for example, education and persuasion) and scope for remedial action that is not based on individual action. Depending on how they are structured, they may include regulators with broad powers, including powers to conduct own motion investigations and to provide compensation, as well as civil and criminal penalties for more egregious or harmful conduct. They therefore offer broad scope for a regulatory solution that incorporates a pyramid of enforcement measures; one which can be tailored to address both the private and the broader public harms created by untrammelled public place surveillance.

VII. A Suggested Way Forward

The flexibility inherent in data protection regimes suggests that they offer the best starting point for regulation of surveillance, provided that they include independent regulators who have a range of softer and harder enforcement powers at their disposal and who are both able, and prepared to make use of, their more coercive powers in those instances where the softer measures have failed to elicit compliance. As noted by Ayers and Braithwaite:

> [T]he greater the heights of tough enforcement to which the agency can escalate (at the apex of its enforcement pyramid), the more effective the agency will be at securing compliance and the less likely that it will have to resort to tough enforcement. Regulatory agencies will be able to speak more softly when they are perceived as carrying big sticks.[137]

It is also important to find means of addressing the weaknesses identified above, and especially the issue of PII. As noted above, whether or not information qualifies as PII provides the touchstone for the application of an entire set of FIPs, including limitations on collection, use and disclosure, security requirements and obligations to provide rights of access and amendment. Their wording and interpretation therefore remain a matter of continuing controversy.

A prime example is the decision of the United Kingdom Court of Appeal in *Durant v Financial Services Authority*,[138] in which the expression "personal data" in the *Data Protection Act*[139] was interpreted as requiring an assessment of relevance or proximity to an individual. This, in turn, required assessment of whether the information is "biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations";[140] and whether it has "the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest".[141]

This test has been legitimately criticised on the basis that it eliminates the key obligations imposed under the *Data Protection Act*, including "fair processing, data security and no unreasonable data retention" as well as the rights of persons whose images are collected to control how they

137. *Ibid* at 6.
138. [2003] EWCA Civ 1746 [*Durant*].
139. *Data Protection Act 1988* (UK), c 29.
140. *Durant*, *supra* note 138 at para 28.
141. *Ibid*. See further Lilian Edwards, "Taking the 'Personal' Out of Personal Data: *Durant v FSA* and its Impact on the Legal Regulation of CCTV" (2004) 1:2 Script-ed 346.

are processed.[142] However, it is arguable that the test made sense in the context of the specific situation in which the applicant was requesting access to all documents in which he was featured and that the preferable way forward is to incorporate different tests based on the specific practices that are in issue and their potential privacy implications for information subjects.

Schwartz and Solove take a similar approach in arguing for reconceptualization of PII tests to resolve the reidentification issues identified by Ohm. They propose the development of a new model termed "PII 2.0", which provides different regulatory regimes for information about identified and identifiable individuals.[143] They suggest that, while all of the FIPs should apply to information about identified individuals, only some should apply to identifiable data.[144] They further suggest that "[f]ull notice, access, and correction rights should not be granted to an affected individual simply because identifiable data about her are processed" and also that "limits on information use, data minimalization, and restrictions on information disclosure should not be applied across the board to identifiable information".[145]

This suggests a useful way forward, although the distinction between identified and identifiable is a blunt one and fails to answer the question: identified by whom and in what circumstances? What is important at the end of the day is whether or not data collected is handled in ways that pose an actual or potential threat to the data subject.

Take, for example, the hypothetical scenario of a marine researcher who incidentally captures images of Angelina Jolie on a boat when collecting images of wave movements from a fixed camera. It is arguable that the researcher should not be subject to collection limitation, access and amendment principles, although they should be required either to redact the images or to hold them securely. On the other hand, the researcher

142. Lilian Edwards, "Switching Off the Surveillance Society? Legal Regulation of CCTV in the United Kingdom" in Nout, de Vries & Prins, *supra* note 90 at 101.

143. Schwartz & Solove, *supra* note 76.

144. *Ibid*.

145. *Ibid* at 1880.

should be subject to a broader range of principles if he or she wishes to use the images or disclose them to others. The key objective of this approach is to ensure that data that can potentially identify an individual receives protection only where necessary to protect the individual's privacy and also to provide an incentive to organisations to deidentify or destroy such data where it is not collected for the purpose of collecting information about the individual. It is important to remember that the appropriate disposal of personal data once it is no longer required for the purposes for which it was collected is fundamental for the protection of privacy, although it strikes at the underlying rationale of the Big Data movement.

Departure from the current "one size fits all" approach may also provide a useful way forward in dealing with the problem that the use of privacy invasive technology is no longer the sole domain of governments and business organisations. FIP-based regimes are currently ill-suited to the regulation of the non-business activities of individuals. However, there may be scope for the development of a more simplified set of principles that focus on privacy invasive uses and disclosures of personal information.

A second major issue identified by Cate is that most FIP-based regimes rely heavily on notice and content requirements, resulting in "an avalanche of notice and consent requirements" that are generally ignored.[146] He has therefore proposed an alternative set of rules based on principles of harm prevention, benefit maximisation and consistent protection.[147] Building on this approach, Cate, Cullen and Schonberg have proposed a revised set of OECD Guidelines, which have been informed by a working group organised by the Oxford Internet Institute on behalf of Microsoft.[148]

Cate's approach is to try and shift the emphasis away from control by data subjects and onto accountability on the part of the organisation

146. Cate, "Fair Information Practice Principles", *supra* note 80 at 361.
147. *Ibid* at 370–74.
148. Fred H Cate, Peter Cullen & Victor Mayer-Schönberger, "Data Protection Principles for the 21st Century: Revising the 1980 *OECD* Guidelines" *Oxford Internet Institute* (March 2014), online: OII <www.oii.ox.ac.uk/news/?id=1013>.

involved in handling personal data. It also, however, reduces existing limitations on the secondary uses of data and imposes regulation only to the extent that information handling is clearly harmful to information subjects. In that sense, it shifts the balance in favour of Big Data while retaining a safety net to catch activities that are clearly harmful and disproportionate in their privacy invasiveness.

This development has been criticised by Cavoukian, Dix and El Eman[149] on the basis that diluting consent requirements weakens privacy protection. They acknowledge the modern reality that individuals are not only confused by lengthy privacy notices but often also unaware of the data collection taking place or that they may be completely absent from the transaction which requires the processing of their data. However, they point out that depriving individuals of control over the purposes for which their personal data is collected and used is not beneficial to them; "it makes them vulnerable to the judgement exercised by others — corporate and bureaucratic systems that already affect our lives, and over which we have little or no control".[150] They also highlight that "greater reliance on law and regulation alone to police "after-the-fact" abuses of personal data is a misguided strategy; and … that there is little consensus on defining "harms" or ways in which to measure or mitigate privacy harms".[151]

Cavoukian and her co-authors suggest instead "a more robust user-centric "Transparency and Control" model"[152] based on seven principles of "Privacy by Design". Their concept of "Privacy by Design" is based on the view that "[p]rivacy and data protection should be incorporated into networked data systems and technologies by default, and become integral to organizational priorities, project objectives, design processes, and

149. Canada, Information and Privacy Commissioner, *The Unintended Consequences of Privacy Paternalism*, by Ann Cavoukian, Alexander Dix & Khaled El Emam (Toronto: 5 March 2014), online: University of Toronto <www.comm.utoronto.edu/~dimitris/JIE1001/levin4.pdf>.

150. *Ibid* at 4.

151. *Ibid* at 2.

152. *Ibid* at 13.

planning operations".[153] "Privacy by Design" has the advantage that it imposes responsibility on those involved in the collection and processing of data to build in measures to protect the privacy of individuals and is embodied as a requirement in the *General Data Protection Regulation*, which will commence operation in the European Union in May of 2018.[154] However, there is still a lack of clarity as what precisely this concept requires, and there are difficulties in implementing it in a context where it is inherently difficult to reconcile privacy interests with the interests of the Big Data movement.

A different approach based on the so-called "Right to be Forgotten" involves conferring on individuals specific rights to require the erasure of their personal information.[155] This has some potential to restore some measure of control to the individual and is embodied as a requirement in the *General Data Protection Regulation*.[156] However, a key shortcoming is that it relies on the individual for enforcement. This is problematic in a context where individuals are unaware of what information has been collected about them and how it is being used.

It is suggested that a different approach which may hold promise, is to improve the transparency not just of the different aspects of information handling but also of the outcomes of that process. The process of modulation described by Cohen[157] is harmful, at least in part, because

---

153. *Ibid* at 15.
154. EC, *Data Protection Regulation (EC) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [*General Data Protection Regulation*]. It is required under art 25 in respect of "potentially high-risk processing activities".
155. For a useful discussion of the advantages of such a right, see Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009).
156. *General Data Protection Regulation*, *supra* note 154. Article 17 confers a right of erasure in specific circumstances, including where the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
157. Cohen, "What Privacy is For", *supra* note 30.

of its normalisation and the fact that individuals are unaware of the extent to which they are being manipulated. The provision of additional information at that stage (for example, informing individuals who are the subject of targeted advertising of why it is that they are receiving specific advertisements) might go some way towards alleviating these issues.

Providing increased transparency creates practical difficulties that are magnified in the context of activities based on Big Data Analytics, due to the complexities associated with making transparent the algorithms that are used to inform those activities. However, the fact that this task is difficult does not mean that it should not be attempted given the seriousness of the potential harm involved. Improving the transparency of the end products of surveillance arguably has the potential to produce more informed decision-making on the part of individuals than notices given at the point of information collection.

"A Virtual 'Puppet'": Performance and Privacy in the Digital Age

Megan Richardson*

The recent case of Garcia v Google *identifies a central problem of the internet world as we know it — that speech may be freer and more powerful than before and opportunities for creative expression radically extended but individuals may lose control over what happens to their images and other distinctive features, challenging assumptions about their identity. In the discussion below, it is argued that the time has come to move beyond relying on the language of "privacy" and if the idea is to allow individuals to maintain control over the formulation of personal identity in the digital age, then laws should be framed around that.*

* Professor of Law and Joint Director, Centre for Media & Communications Law, The University of Melbourne.

I. Introduction
II. Nebulous Privacy
III. Reputation Insufficient
IV. Towards a Right to Identity
V. Conclusion

I. Introduction

A curious moment in the case of *Garcia v Google Inc.* was the passing comment of Judge Margaret McKeown that "[p]rivacy laws, not copyright, may offer remedies tailored to Garcia's personal and reputational harms".[1] My initial reaction was to wonder what privacy interests were at stake in this case of Innocence of Muslims whose trailer aired on YouTube in 2012, fomenting outrage across the Muslim world, violent protests in the Middle East and parts of Asia (where it was blocked)[2] and Australia (where it was not),[3] and a fatwa issued from an Egyptian cleric against those associated with the film including its performers.[4] Cindy Lee Garcia's complaint before the 9th Circuit was that she was deceived into thinking that the film, originally titled Desert

1. *Garcia v Google, Inc.*, 786 F (3d) 733 at 745 (9th Cir 2015) (en banc) (US) [*Garcia v Google*].
2. See Jeremy Bowen, "Anti-Islam Film: Thousands Protest around Muslim World" *BBC News* (17 September 2012), online: BBC <www.bbc.com/news/world-middle-east-19625167>.
3. "As it Happened: Violence Erupts in Sydney over Anti-Islam Film" *ABC News* (16 September 2012), online: ABC <www.abc.net.au/news/2012-09-15/anti-us-protests-hit-sydney/4263372>.
4. See Andrew Blankstein & Ned Parker, "Police Probe Threats, Fatwa against "Innocence of Muslims" Actors" *Los Angeles Times* (21 September 2012), online: LA Times <latimesblogs.latimes.com/lanow/2012/09/police-probe-threats-fatwa-against-innocence-of-muslims-actors.html> (adding "[w]hether anyone will abide by them is another matter. Senior mainstream Sunni clerics have urged restraint in regard to the film").

Warrior, was to be an historical Arabian Desert adventure film.[5] Instead, during post-production it was turned into an anti-Islamic polemic, with her lines overdubbed to express the director's "hateful" "bigoted" views, using her as a virtual "puppet" in a manner repugnant to her character as someone who would "never debase another person's religious beliefs".[6] Further, the instrumentalities of the film's notoriety, Google and YouTube, refused to take it down despite her many requests relying on the *Digital Millennium Copyright Act*.[7] As a result of these acts and refusals, Garcia claimed, she suffered emotional distress, the destruction of her career and reputation and credible death threats.[8] It seems that, at this point of the proceedings, copyright not privacy was Garcia's legal concern. Yet for fairly obvious reasons to do with the fact that copyright law protects authors not performers, that claim failed,[9] leaving Garcia with no legal claim — subject to the puzzling hint above that had she pursued an alternative claim in privacy she might yet have prevailed. And I am still puzzled. Yes, there are a number of scenarios where privacy laws

---

5. She was not the only one. Other actors also maintained that they were duped by Nakoula into thinking the film was an incompetent amateur adventure story although admittedly they did not look too closely. See Michael Joseph Gross, "Disaster Movie" *Vanity Fair* (27 December 2012), online: Vanity Fair <www.vanityfair.com/culture/2012/12/making-of-innocence-of-muslims>.
6. See Garcia's Complaint in *Cindy Lee Garcia v Nakoula Basseley Nakoula*, *et al*, 2012 WL 4426549 at paras 4, 8–9, 29 (CD Cal 2012) (US) [Garcia's Complaint, CD Cal].
7. 112 Stat 2860 (US).
8. Garcia's Complaint, CD Cal, *supra* note 6 at para 38; *Garcia v Google*, *supra* note 1 at 745.
9. *Garcia v Google*, *ibid* at 742–745. For a thorough analysis of the different stages of the case, including an earlier judgment for Garcia given by Judge Kozinski in the 9th Circuit in *Garcia v Google, Inc* 766 F (3d) 929 (9th Cir 2014) (US), overturned by the en banc Court (Judge Kozinski dissenting), see Elizabeth Martin, "Using Copyright to Remove Content: An Analysis of *Garcia v Google*" (2016) 26:2 Fordham Intellectual Property, Media and Entertainment Law Journal 464. Documents for the case are available at *Santa Clara Law Digital Commons*, online: SCU <https://digitalcommons.law.scu.edu>.

rather than copyright might be the preferable basis for a claim, especially if copyright is restricted to protecting and fostering authored creative expression as the 9th Circuit posited in Garcia's case,[10] echoing an argument of Samuel Warren and Louis Brandeis in 1890.[11] And we can debate whether, nevertheless, if privacy law fails to provide an effective remedy in such cases, copyright and other claims may be drawn on to fill the gap.[12] But what was the "digital circuit"[13] signalling with its suggestion that privacy should frame the response to the essential problem that Garcia identified in her case? The problem of individuals caught up as "puppets" in fictionalised worlds created and fostered by others working behind the scenes and pursuing their own ends — the internet world as we know it, where speech may be freer and more powerful than before and opportunities for creative expression radically extended but individuals may lose control over what happens to their images and other distinctive features, challenging assumptions about their identity? In the discussion below, I argue that the time has come to move beyond relying on the nebulous language of "privacy" and if the idea is to allow individuals to

10. *Garcia v Google*, *ibid* at 745. See further the Hon Margaret McKeown, "Censorship in the Guise of Authorship: Harmonizing Copyright and the First Amendment" (2016) 15:1 Chicago Kent Journal of Intellectual Property 1.
11. Samuel Warren & Louis Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193 at 205.
12. See, for instance, Margaret Chon, "Copyright's Other Functions" (2016) 15:2 Chicago Kent Journal of Intellectual Property 364 (giving the particular example of "cyber-harassment [using] non-consensual pornography" at 366). In fact remedies may not be limited to copyright to deal with such cases. See Federal Trade Commission, Press Release, "Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos" (29 January 2015), online: FTC <www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges>; and Danielle Citron & Woodrow Hartzog, "The Decision That Could Finally Kill the Revenge-Porn Business" *The Atlantic* (2 February 2015), online: The Atlantic <www.theatlantic.com/technology/archive/2015/02/the-decision-that-could-finally-kill-the-revenge-porn-business/385113/>.
13. The label adopted by the Hon McKeown, *supra* note 10 at 1.

maintain control over the formulation of personal identity in the digital age, then laws should be framed around that.

II. Nebulous Privacy

Even a superficial examination of Garcia's privacy claims in her earlier proceeding before the Superior Court of the State of California, later to be superseded by her federal proceeding, shows the challenges of claiming privacy in a case such as this.[14] Garcia claimed invasion of her constitutional right to privacy under the California Constitution,[15] again using the imagery of "a virtual 'puppet'" to object to Nakoula Basseley Nakoula's treatment of her as an "egregious breach of social norms",[16] and false light invasion of privacy under California law;[17] namely, that "Defendants, through the above described Film and their actions in publishing it, including the contents that falsely purported to depict Plaintiff saying bigoted things that she did not say, gave publicity to matters concerning Plaintiff that unreasonably places her in a false light and violates her right to privacy".[18] Yet these claims, along with claims for fraud, unfair business practices, right of publicity, defamation and intentional infliction of emotional distress were discontinued after the Superior Court dismissed the application for a preliminary injunction

14. Complaint of Cindy Lee Garcia in *Cindy Lee Garcia v Nakoula Basseley Nakoula, et al*, Case No BC 492358, filed Superior Court, County of Los Angeles, State of California, September 19, 2012 [Garcia's Complaint, Sup Ct].
15. Although query whether the Constitution could in itself provide the basis for a claim as opposed to lending constitutional support and weight to a claim, as in *Melvin v Reid*, 112 Cal App 285 (Ct App 1931) (US), where the Constitutional right to privacy was said to support the plaintiff's common law tort claim of the defendant's public disclosure of private facts when it identified her as the subject of its film biopic about her former life as a prostitute swept up in a murder trial.
16. Garcia's Complaint, Sup Ct, *supra* note 14 at paras 24, 26.
17. See William Prosser, "Privacy" (1960) 48:3 California Law Review 383 at 398–491, identifying false light as the third of four torts developing in the wake of Warren & Brandeis's article, Warren & Brandeis, *supra* note 11, recognised in states including California.
18. Garcia's Complaint, Sup Ct, *supra* note 14 at para 30.

on the basis that "Plaintiff has not shown a likelihood of success on the merits".[19] Presumably this was because she was unable to demonstrate that the absent Nakoula had acted falsely and with "actual malice", that is with knowledge of falsity or reckless disregard of truth or falsity,[20] her Constitutional burden in this case of a newsworthy publication according to the Supreme Court in *Time, Inc v Hill*.[21] Moreover, given she was applying for a mandatory injunction, a prior restraint, asking "that the offending content be removed from the Internet",[22] her burden was especially high. We can imagine the Superior Court at this preliminary stage thinking there might have been a variety of possible exonerations of Nakoula's conduct, including that Garcia had signed the usual release

19. See *Cindy Lee Garcia v Nakoula Basseley Nakoula, et al*, Case No BC 492358, filed Superior Court, County of Los Angeles, State of California, September 19, 2012 [Minutes of Garcia's Complaint, Sup Ct], specifically Judge Luis A Lavin, minutes entered 20 September 2012.
20. Garcia unsuccessfully sought to argue "actual malice" in these terms in her Complaint. See Garcia's Complaint, Sup Ct, *supra* note 14 at para 36.
21. *Time, Inc v Hill*, 385 US 374 (1967) [*Time, Inc*], another false light claim where the plaintiff argued that the defendant's theatre review of a Broadway play misrepresented the play's fictionalised account of a home invasion as the actual home invasion which the plaintiff and his family had suffered. Also see Andrew T Kenyon & Megan Richardson, "Reverberations of Sullivan" in Andrew T Kenyon, ed, *Comparative Defamation and Privacy Law* (Cambridge: Cambridge University Press, 2016) ch 16.
22. Garcia's Complaint, Sup Ct, *supra* note 14 at para 11.

form that performers signed for films,[23] or impliedly consented to his post-production editing through her participation in the film (as the District Court later held in her federal case,[24] a finding that the 9th Circuit was reluctant to disturb as "clearly erroneous", notwithstanding its conclusion that she was "bamboozled").[25] Thus, even apart from the problem that Google/YouTube were immunised from liability under Section 230 of the *Communications Decency Act*[26] ("*CDA*"), as Rebecca Tushnet points out,[27] her prospects of success under her State law privacy claims seemed to be weak at best.

As such, Judge McKeon's suggestion that privacy laws might have been a better avenue to give Garcia a viable claim to address her "personal

23. As Nakoula later argued in the federal proceedings: see Declaration of Timothy L Alger for Google and YouTube, *Garcia v Google*, *supra* note 1. The Release appended specifically grants to "Sam Bessi" and his production entity the right to photograph and record Ms. Garcia, releases all claims including for invasion of privacy, right of publicity or other civil rights in connection with the authorized use of her likeness and sound in the film and assigns the rights necessary to make the film (including any relevant copyright, performance right or right of publicity). See also Nakoula's Answer, filed on 20 May 2014, *Garcia v Google*, *supra* note 1 at 1–2, which alleges not only that Garcia signed the Release but states that the words spoken by her character in *Innocence of Muslims* "came from her voice and were never changed", adding that "any NON-UNION actress such as the Plaintiff knows that any movie they participate in represents the opinions or knowledge of the writers and Producers, not the actors". Garcia nevertheless disputed the authenticity of the document with the support of a handwriting expert: See Declaration of James A Blanco (handwriting expert), filed 30 November 2012, *Garcia v Google*, *supra* note 1.
24. See Order of Judge Michael W Fitzgerald that denies Plaintiff Garcia's Motion for Preliminary Injunction in *Cindy Lee Garcia v Nakoula Basseley Nakoula, et al*, 2012 WL 12878355 (CD Cal 2012) (US) [2012 Order Denying Garcia's Motion].
25. *Garcia v Google*, *supra* note 1 at 736, 737, 743 (incongruously finding that Garcia was "bamboozled" and lines were "dubbed", yet the District Court was not clearly erroneous in finding she impliedly consented).
26. 47 USC tit V § 230.
27. Rebecca Tushnet, "Fair Use's Unfinished Business" (2016) 15:2 Chicago Kent Intellectual Property 399.

and reputational harms" than copyright is rather surprising. Nevertheless the question whether privacy is the appropriate organising principle and theoretical foundation of a false light claim,[28] offering a powerful argument based on dual ideas of human dignity and individual flourishing as core principles of a liberal society,[29] is still worth considering. So, was *Garcia v Google* even a case about privacy? If I take as the core concern of privacy the desire to be "let alone", as Warren and Brandeis put it in 1890,[30] or not to be subjected to the "public gaze" as Lisa Austin explains,[31] then I would say no. Further, stretching the meaning of privacy to cover Garcia's situation, treating privacy in a "pluralist manner from the bottom up", as Daniel Solove for instance argues,[32] would only undermine this important idea. The difficulty is not that Garcia is a performer and lives much of her life in the public gaze. For even performers and those who live much of their lives in the public gaze can benefit from periods "backstage" in

28. See Melville Nimmer, "The Right to Speak from Times to Time: First Amendment Theory Applied to Libel and Misapplied to Privacy" (1968) 56:4 California Law Review 935; *Cf.* Dianne Zimmerman, "False Light Invasion of Privacy: The Light that Failed" (1989) 64:2 New York University Law Review 364 (although doubting that the claim has anything to do with privacy).
29. Warren & Brandeis, *supra* note 11, talk about both dignity and flourishing: the right to privacy a right of "inviolate personality" at 205; development of an "intense intellectual and emotional life" the product of "the advance of civilisation" which law must respond to, at 195, although the first is more prominent. See also Edward J Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39:6 New York University Law Review 962; Nimmer, *ibid* at 959.
30. Warren & Brandeis, *supra* note 11 at 195; see also 196 (as opposed to "intrusion upon the domestic circle").
31. Lisa Austin, "Privacy and the Question of Technology" (2003) 22:2 Law & Philosophy 119.
32. Daniel Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008), proposing a pluralist theory of privacy in these terms at 40; and treating false light as falling within a privacy taxonomy "because of its significant similarity to other privacy disruptions", involving "the spreading of information that affects the way society views a person" and resulting in "embarrassment, humiliation, stigma, and reputational harm" at 160.

order to relax with close associates, prepare for the "putting on and taking off of character", engage in informal and intimate conduct, and find opportunities for reflection as well as support from peers, as Canadian sociologist Erving Goffman pointed out in his study on *The Presentation of the Self in Everyday Life* some sixty years ago.[33] And those of us who find that being onstage is a near-constant feature of modern internet life can draw a similar conclusion about the importance of privacy. Yet Garcia showed no sign of this being her desire in this particular instance. Rather, her objection to being used as a "virtual puppet" seemed to have more to do with another common human desire talked about by Goffman, namely that of maintaining control over the "frontstage" performances in different aspects of one's everyday life.[34] As such, it is hard to see this as a false light right to *privacy* claim (although such arguments may be more feasible in some other false light cases, such as *Time, Inc v Hill* where the claimed false light publicity concerned matters that were private family matters which the plaintiff would rather not have seen aired in public).[35]

III. Reputation Insufficient

On the other hand, query whether reputation is necessarily a preferable organising principle as some, including William Prosser, have argued.[36] Yet perhaps it comes closer than privacy in many cases. It has the beneficial

33. Erving Goffman, *The Presentation of Self in Everyday Life* (Garden City: Anchor Books, 1959) ch 3 at 120–130, passim [Goffman, *Presentation of Self*].
34. See *ibid*, ch 1, where Goffman talks about the challenges of impression management, the need to negotiate different roles, the difficulty of maintaining expressive control, and the risks of being caught out.
35. As Nimmer argues, *supra* note 28 at 962–66 (although Zimmerman doubts this, *supra* note 28 at 432–34). See similarly, regarding the UK's tort of misuse of private information, *McKennitt v Ash*, [2006] EWCA Civ 1714, Longmore LJ ("[t]he question in a case of misuse of private information is whether the information is private not whether it is true or false" at 86).
36. Prosser, *supra* note 17 ("the interest protected is clearly that of reputation" at 400).

feature of being concerned with the frontstage aspect of a performance.[37] And as Justice Stewart said in *Rosenblatt v Baer*, "the right of a man to the protection of his own reputation from unjustified invasion and wrongful hurt reflects no more than the basic concept of the essential dignity and worth of every human being — a concept at the root of any decent system of ordered liberty".[38] Thus, while I might dispute whether the false light tort can be wholly equated the protection of reputation in every case (for instance, recall the *Time, Inc v Hill* case noted above), the concerns may be more along these lines in some cases. Was this the case for Garcia who in her false light claim talked of "being shunned, avoided and subjected to ridicule", resulting in "significant damage to her reputation and to her livelihood", harms usually associated with defamation and repeated in her defamation claim?[39] The 9th Circuit at one point suggested that defamation law might equally be an appropriate claim to address Garcia's "personal and reputational harms".[40] Not that her prospects of a remedy were greater with defamation, given the "actual malice" standard equally applies,[41] prior restraints are equally resisted, and Section 230 of the *CDA* extends to such claims (and recall that Garcia's defamation claim was dismissed by the Superior Court along with her privacy claims; moreover, she suffered the same result in the District court where a defamation

37. See Warren & Brandeis, *supra* note 11 at 197. Warren and Brandeis distinguish reputation from privacy, identifying this as essentially concerning "the individual in his external relations to the community, by lowering him in the estimation of his fellows" (as opposed to "intrusion upon the domestic circle" which is they identify as a core concern of privacy as a right to be "let alone").
38. *Rosenblatt v Baer*, 383 US 75 at 92 (1966) [*Rosenblatt*].
39. Garcia's Complaint, Sup Ct, *supra* note 14 at paras 30, 33, 34, 69, 76.
40. *Garcia v Google*, *supra* note 1 at 741, 745.
41. Indeed, the Court in *Time, Inc*, *supra* note 21, in setting out an "actual malice" test followed the path being established for defamation in *New York Times Co v Sullivan*, 376 US 254 (1964) (where the standard was applied to public officials); *Curtis Publishing Co v Butts*, 388 US 130 (1967); *Associated Press v Walker*, 389 US 28 (1967); *Gertz v Robert Welch, Inc*, 418 US 323 (1974) (where the standard was extended to public figures). See Kenyon & Richardson, *supra* note 21.

claim was added to her copyright claim).[42] But there is a suggestion here that defamation and false light may be rather alike in their treatment of reputational harms, although from Garcia's perspective there seemed to be some differences. Her false light claim focussed more on personal harms and invoking the moral standard that the conduct was "highly offensive to a reasonable person".[43]

Of course it may still be argued that such personal harms can be brought within the rubric of a defamation claim broadly construed and generously applied. And in common law jurisdictions such as the United Kingdom, Australia, and Canada which do not recognise a false light tort, a distinctly American invention, a claimant in Garcia's position would probably rely on defamation to address her personal and reputational harms[44] (possibly supplementing this with reference to the right to reputation under the *European Convention on Human Rights*[45] in

42. See Minutes of Garcia's Complaint, Sup Ct, *supra* note 19; 2012 Order Denying Garcia's Motion, *supra* note 24.
43. See Garcia's Complaint, Sup Ct, *supra* note 14 at para 31 ("[t]he false light in which Plaintiff was placed would be highly offensive to a reasonable person"), and para 33 ("[p]laintiff has suffered and will suffer emotional distress, and has been, and continues to be, embarrassed and humiliated by the false statements and implications, [and] terrorized by the death threats that she has received as a result of the false light in which she has been placed...").
44. See *Youssoupoff v Metro-Goldwyn-Mayer Pictures Ltd* (1934), 50 TLR 581 (CA (Eng)) (substantial damages awarded to plaintiff Princess Youssopov who claimed defamation in her portrayal as a fictional character in the film *Rasputin, the Mad Monk*); *Kidu v Fifer*, [2016] NSWSC 488 (Austl) [*Kidu*, 2016] (granting an interlocutory injunction against defendant filmmaker showing certain extracts from her film at a Canadian festival after the subject who signed a release then purported to withdraw it), although the plaintiff's version of the facts of the parties' agreement was successfully disputed and the injunction discharged in *Kidu*, 2016.
45. *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) [*ECHR*].

the UK).[46] Further, given that reasonableness rather than "actual malice" is the touchstone of analysis in these jurisdictions,[47] the claim might well succeed. Indeed, an injunction might be awarded, based on recent experience of an injunction granted in the Irish internet defamation case of *McKeoh v John Doe* where the plaintiff was falsely identified as a taxi fare evader and subjected to public condemnation, after an attempt on the part of the court to broker a voluntary arrangement with Google and Facebook to take appropriate steps failed.[48] Thus it may be said that the right to reputation is better recognised in these jurisdictions than in the US, providing an effective vehicle to deal with false light-type claims in cases where a privacy claim is unavailing.[49] Nevertheless, the point remains that an exclusive focus on reputation where privacy is unavailing risks understating the personal dimension of a false light claim — that while "reputation" may be understood broadly as "the estimation by which the community holds a person",[50] or "the social apprehension that we have of each other" as Robert Post puts it,[51] focussing just on the way that a person is judged by their community risks fails to appreciate Goffman's point that multiple diffuse aspects may contribute to a performer's success (or failure) in projecting an identity, or "self", including the way that "the

46. See Tanya Aplin & Jason Bosland, "The Uncertain Landscape of Article 8 of the ECHR: The Protection of Reputation as a Fundamental Human Right?" in Kenyon, *supra* note 21, ch 13.
47. See, for instance, *Jack Monroe v Katie Hopkins*, [2017] EWHC 433 (QB) (allegation by defendant right-wing blogger that plaintiff left-wing blogger had vandalised a war memorial); *Rebel Wilson v Bauer Media*, [2017] VSC 521 (Austl) (allegation in *Women's Day* based on email correspondence with anonymous source that plaintiff actor was a serial liar); *Baglow v Smith*, 2015 ONSC 1175 ("more vocal supporters" although there treated as "fair comment" on the basis they were statements of opinion not fact).
48. *Eoin McKeogh v John Doe*, [2012] IEHC 95 (HC (I)), specifically decision of Peart J on Interlocutory Injunction application.
49. Although this is not to say that a privacy claim would not be viable in some cases, see *Rosenblatt*, *supra* note 38.
50. See Aplin & Bosland, *supra* note 46 at 268.
51. Robert C Post, "The Social Foundations of Defamation Law: Reputation and the Constitution" (1986) 74:3 California Law Review 691 at 692.

individual … handle[s] things during his presence among others".[52] Here having a strong sense of identity may count for more than reputation.

IV. Towards a Right to Identity

Thus my argument is that we should consider a right to identity as an appropriate frame for false light cases in the internet world where so much more is social than before. A focus on identity would take us beyond considerations of reputation and also privacy in assessing the harms suffered by a person in a false light case, even appreciating that reputation and privacy may be relevant as well and may sometimes coincide (for instance, where a person is affected in their private self by the judgments of others). It would allow us to consider what Jeremy Waldron refers to as a "concern for the ordinary dignity of an individual focus[ed] on the ways his or her status is affirmed and upheld — and the ways in which it might be endangered — as one person among thousands or millions of

52. *Ibid*, citing Erving Goffman, *Interaction Ritual* (Garden City: Anchor Books, 1967) [Goffman, *Interaction Ritual*] talking about a person's "projected … identity" or "self" (or "selves") as a product of various things including reputation (the way that a person may be remembered and judged from the past), social role and status, and more particular factors such as setting, audience and (most significantly here) the ways that "the individual … handle[s] things during his presence among others" at 107–108, 168.

others",[53] and having to do with the person's capacity to engage effectively in public discourses and contribute to the formulation of a diverse multi-vocal community.[54] As Waldron puts it, there is "a sort of public good of inclusiveness that our society sponsors and that it is committed to"[55] — using language reminiscent of Goffman's earlier observation that in "urban secular living", the individual "walks with some dignity", aware of his "status" relative to those of others and "finding that they must treat him with ritual care", but now adapting this idea to suit a modern virtual setting where "status" is a more fluid thing than previously imagined and a person's ability to maintain their identity is key.[56] This sentiment comes through in Garcia's complaint that her identity as an individual who

53. Jeremy Waldron, *The Harm in Hate Speech* (Cambridge, MA: Harvard University Press, 2012) at 142 [Waldron, *Harm in Hate Speech*] in Jeremy Waldron, "How Law Protects Dignity" (2012) 71:1 Cambridge Law Journal 200 at 202 [Waldron, "How Law Protects Dignity"], Waldron expands on the concept he is putting forward here of a dignitarian "status" as "predicated on the fact that [the person] is recognised as having the ability to control and regulate her actions in accordance with her own apprehensions of norms and reasons that apply to her; it assumes that she is capable of giving and entitled to give an account of herself (and of the way in which she is regulating her actions and organising her life), an account that others are to pay attention to; and it means finally that she has the wherewithal to demand that her agency and her presence among us as a human being be taken seriously and accommodated in the lives of others, in others' attitudes and actions towards her, and in social life generally". See also Jeremy Waldron, "Lecture 2: Law, Dignity, and Self-Control" in Jeremy Waldron, *Dignity, Rank, and Rights* (Oxford: Oxford University Press, 2012).
54. See especially Waldron's discussion in *The Harm in Hate Speech*, *ibid* at 4–5, 58–60, talking about hate speech. Waldron's terms this group defamation but I think it goes beyond defamation designed simply to protect reputation.
55. *Ibid* at 4.
56. Goffman, *Interaction Ritual*, *supra* note 52 at 95. Generally in a more traditional way Goffman connects status more with a person's position in society, *e.g.* a person of higher or lower status — but in this quoted comment he hints at a more flexible evolving idea of social status more reminiscent of Waldron's.

would "never debase another person's religious beliefs" was being radically impugned by Nakoula's egregious breach of social norms, combined with the unwanted notoriety conferred by Google/YouTube's worldwide publication.[57] As such, we have a powerful argument against the argued rights of those such as Nakoula, Google and YouTube to engage in free speech without restraint,[58] based on an individual's ability to express herself freely on her own terms, participate in public discussions and democratic processes, and even possibly avoid violence and maintain truth in an environment in which she is accurately represented.[59]

I appreciate that this reasoning would represent a shift beyond Warren and Brandeis's advocacy of a right to be "let alone" as but one aspect of what they called "inviolate personality",[60] coming closer to a right in inviolate personality. But then the false light tort already takes us beyond the right to privacy, as Prosser points out.[61] I believe it would also take us further than a right to reputation, although this is also important, and may be almost enough in a case such as Garcia's. If anything, it comes closest to the right of publicity which is sometimes couched as a

57. See Garcia's Complaint, CD Cal, *supra* note 6; Garcia's Complaint, Sup Ct, *supra* note 14.

58. See Nimmer, *supra* note 28 at 949–950, summarising the values of free speech as elucidation of truth, democratic participation, self-expression and aversion of violence, citing, *inter alia,* Justice Brandeis in *Whitney v California*, 274 US 357 at 375–377 (1927). Although query whether violence was averted by publication of *Innocence of Muslims*.

59. Including the prospect of violence against Garcia. Note, however, the argument of Judge Watford in *Garcia v Google* that "[t]he sad but unfortunate truth is that the threat posed to Garcia by issuance of the fatwa will remain whether *The Innocence of Muslims* is available on YouTube or not. Garcia is subject to the fatwa because of her role in making the film, not because the film is available on YouTube": *Garcia v Google*, *supra* note 1 at 748. But perhaps a different kind of injunction, such as a public disclaimer of association available on YouTube, might be more effective here.

60. See Warren & Brandeis, *supra* note 11 at 205.

61. See Prosser, *supra* note 17.

way of protecting a person's "identity" from commercial appropriation.[62] But I am not suggesting that false light amounts to a full appropriation of identity, in the sense of taking over a person's identity.[63] Rather, I am simply arguing that the law here should offer protection from an unjustifiable attack on a person's identity, specifically her perception of herself as someone who has the "ability to control and regulate her actions in accordance with her own apprehensions of norms and reasons that apply to her", as Waldron puts it.[64] Nor am I going as far as to advocate a European-style right to control the use of personal information, a right also based on an idea of a right to personality which transcends privacy and reputation and may go significantly further,[65] appealing as that may be in the internet environment where control over personal information may be key to a person's capacity to maintain an independent dignified existence.[66] For present purposes, I am merely making a limited argument that the false light invasion of privacy tort would be better framed as a tort not just about privacy but as also covering reputational and identity

62. See, for instance, Garcia's Complaint, Sup Ct, *supra* note 14 ("California's Right of Publicity Statute, California Civil Code § 3344 et seq, protects persons from the unauthorized appropriation of the person's identity by another for commercial gain" at para 38). Note also as to the common law right of publicity, *Midler v Ford Motor Co*, 849 F 2d 460, 462 (9th Cir 1988) (US) ("California will recognize an injury from 'an appropriation of the attributes of one's identity'", citing *Motschenbacher v RJ Reynolds Tobacco Co*, 498 F 2d 821 (9th Cir 1974) (US)).
63. Query whether the right of publicity, being confined generally to publicity in advertising or trade (as, for instance, under Cal Civ Code § 3344 (US)) should extend to the posting of a film on YouTube, despite Garcia's argument that a commercial or other purpose should suffice.
64. See Waldron, "How Law Protects Dignity", *supra* note 53.
65. As well as providing more effective protection to these rights in some instances where other laws may fall short: for instance, regarding the right to reputation under the ECHR, *supra* note 45, see David Erdos, "Data Protection and the Right to Reputation: Filling the "Gaps" After the Defamation Act 2013" (2014) 73:1 Cambridge Law Journal 536.
66. See Stefano Rodotà, "Data Protection as a Fundamental Right" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne & Sjaak Nouwt, eds, *Reinventing Data Protection?* (Amsterdam: Springer, 2009) ch 3.

harms in ways that egregiously breach social norms about what can and what cannot be deemed to be acceptable within the boundaries of free speech.[67] As such, I believe the tort would not only provide a more appropriate model for dealing with cases such as Garcia's where the essential complaint was the way she was represented publicly, using her as "a puppet", in a manner repugnant to her self-proclaimed identity as someone who would "never debase another person's religious beliefs".[68] It would also provide a useful model for courts in other jurisdictions which from time to time look to US legal innovations in refashioning their laws to better address and deal with the exigencies of modern life.

V. Conclusion

I have argued in this essay that a false light invasion of privacy tort conceived as a way of protecting identity makes the best sense of Garcia's claim in her case against Nakoula, focussing us more sharply on what Garcia alleged to be Nakoula's extreme wrongful conduct in changing the innocent and banal message of Desert Warrior and overdubbing the lines of her character to give it a darker and more dubious role in Innocence of Muslims, exemplified by her repeated complaint that he had treated her as his "puppet", or "virtual puppet", in "an egregious breach of social norms". Perhaps it is no accident that a filmmaker especially would conceive of a character as potentially subject to his dominion and control, and that a performer especially would notice and object to being treated as a puppet? Performance may be a metaphor for the presentation of the self in everyday life, as Goffman has said.[69] But as Garcia's case shows,

---

67. Bearing in mind that the standards of "actual malice", resistance to prior restraints, and s 230 of the *Communications Decency Act,* 47 USC § 230 (1996) would apply and would likely be sufficient to rule out the injunction sought by Garcia, see Garcia's Complaint, Sup Ct, *supra* note 14. Whether that would preclude a more limited injunction, *e.g.* disclaiming her endorsement of Nakoula's views, is another question.
68. See Garcia's Complaint, CD Cal, *supra* note 6; Garcia's Complaint, Sup Ct, *supra* note 14.
69. See Goffman, *Presentation of Self*, *supra* note 33 at 254 (my concern is "the structure of social encounters").

in the expansive theatre of the internet performance and life can easily become blended — and one useful contribution we find in this case is a vocabulary to talk about some of the problems, or as Goffman puts it, "an apt terminology for the interactional tasks that all of us share".[70]

The theatrical terminology also helps us to think about the role assumed by Google and YouTube in all this. In cases such as Garcia's they like to present themselves as merely passive conduits in a production being staged and performed by others for the benefit of an audience, no more than the bricks and mortar of the physical theatre. This is a useful technique in bringing themselves within the terms of Section 230 of the *CDA* which has repeatedly been justified as a bulwark of freedom of speech. And if the value of free speech includes preserving "unpopular speech", as Judge McKeown has said with respect to *Garcia v Google*,[71] then perhaps restraints should not readily be imposed based on the quality of speech. On the other hand, so long as we maintain the position that free speech is justified by values such as individual flourishing, democratic participation, aversion of violence and truth coming out of the market place of ideas, then at very least there needs to be fresh consideration of how those values work in practice. For instance, whether freedom of speech for some people becomes a way of disrupting attempts of other people to fashion their identities, participate in public discussions and democratic processes, avoid violence and maintain truth. Or is it that free speech values are changing? Google/YouTube's policy of publishing everything sometimes makes me wonder whether we are moving into a world where the value of free speech is just free speech. A world of "The Library of Babel", to adopt another metaphor from another sociologist of the post-war period: a world whose disorder repeated over eternity eventually becomes "the Order".[72]

---

70. *Ibid* at 255.
71. Hon McKeown, *supra* note 10 at 16.
72. Jorge Luis Borges, "The Library of Babel" (first published as 'La biblioteca de *Babel' in El jardín de senderos que se bifurcan*. *Sur*, 1941), translated by James E Irby, *Labarynths* (London: Penguin, 2011) at 78, 86.

Information Brokers, Fairness, and Privacy in Publicly Accessible Information

Andrea Slane*

The European Union, Canada, and the United States have each grappled with what counts as fair business practices in relation to information services that collect and package personal information that has ended up in one way or another online. On the open internet, this personal information often originates from two types of online sources: public records like arrests, mugshots, court decisions, and bankruptcy records; and user-generated content hosted on social media platforms and sites. This article argues that personal information that has been exposed to public view — be it by a government institution, another individual or organization, or by the data subject him or herself — should not be considered fair game to any and all subsequent commercial exploitation. The blunt concept of "public" information should be refined to a more nuanced understanding of "publicly accessible" information, where public access can be limited to particular purposes. By focusing on fairness in business dealings in publicly accessible personal information, it should be possible to move beyond a fixation on locating the elusive divide between private and public online information, and instead frame privacy as situated in a three-way balance of interests between the business, the public, and the data subject.

* Andrea Slane, PhD, Associate Professor in Legal Studies, University of Ontario Institute of Technology, Oshawa, Ontario: Andrea.slane@uoit.ca.

I. Introduction
II. The EU's "Right to Be Forgotten" as a Restraint on Commercial Exploitation of Personal Information Online
III. Using Fairness to Restrict Businesses that Facilitate Access to Public Documents Through Information Compilation Products
IV. Businesses that Facilitate and Package User-Generated Content
V. Viral Content: When Online Personal Information Becomes Part of Public Culture
VI. Publicly Available ≠ Free for the Taking
VII. Conclusion: Data Privacy in "Public"

I. Introduction

In the last decade, online information brokers have come under increasing scrutiny from regulators in the European Union, Canada, and the United States. Each jurisdiction has grappled with where to draw the line regarding what kind of business practices are fair in each regime, especially where online businesses provide an information service that includes the collection and packaging of the personal information of individuals whose information has ended up in one way or another online. A comparison of these efforts reveals important variations and policy options, but also some common ground. This article explores these options and the decisions jurisdictions make to restrain the otherwise unimpeded flow of online personal information through information brokers.

Finding appropriate ways to regulate the way personal information flows through commercial business models is necessary, because the choices we make have implications for general commercial fairness in data processing. In particular, it is important to focus on privacy in publicly accessible personal information, since so much personal data is now generated from "public" online activity. This article will focus on recent legal and regulatory developments in the EU, Canada, and the US that deal with information products and services that collect, process, and package publicly accessible personal information. On the open internet, this personal information often originates from two types

of online sources: public records (like arrests, mugshots, court decisions, and bankruptcy records) and user-generated content hosted on social media platforms and sites.

Personal information that has been exposed to public view — be it by a government institution, another individual or organization, or by the data subject him or herself — should not be thought of as fair game to any subsequent commercial exploitation. The blunt concept of "public" information should be refined by shifting to a more nuanced understanding of "publicly accessible" information, where public access to that information can be limited to particular purposes. Each of the three jurisdictions has been engaged in determining what are fair purposes for accessing and subsequently exploiting personal information for commercial gain, albeit in their own distinct ways.

The concept of fairness permeates attempts to restrain commercial exploitation of publicly accessible personal information online. Fairness in business practices as they apply to individuals — whether they be customers or members of the broader public — governs the balance between the value we place in entrepreneurialism and the free market, the right of the public to the benefits provided by those business practices, and the rights of data subjects to be sheltered from certain types and magnitudes of informational harm. By focusing on fairness in business dealings in publicly accessible personal information, it should be possible to move beyond a fixation on locating the elusive divide between private and public online information, and instead frame privacy as situated in a three-way balance of interests among the business, the public, and the data subject.

In the US, efforts to articulate and manage the legitimate flow of personal information online have been spearheaded by the Federal Trade Commission ("FTC"), in particular its enforcement of fair credit reporting obligations and its intervention in unfair and deceptive business practices. In the EU and Canada, these efforts are rooted in data protection regimes that are intended to enforce fair information practices. This article compares how each of the three jurisdictions are working to determine to what extent, and how, existing consumer or data protection regimes should limit the commercial exploitation of

publicly accessible personal information about non-public figures.[1] Part II applies the EU's approach to the "right to be forgotten" as a starting point for exploring fairness in information location service provision, especially with regard to the Court of Justice of the European Union's ("CJEU") characterization of search engines as information brokers (or, in EU Data Protection Directive terms, "data controllers" that process personal information for commercial purposes).[2] Part III discusses how the US and Canada have each dealt with limits on the commercial exploitation of access to public records. Part IV explores how these jurisdictions have dealt with commercial exploitation of user-generated content containing personal information. Part V considers the problem of digital public culture — that is, how to deal with material containing personal information that is popular online, whether as "news" or as viral content like a meme. In an important sense, viral content can become part of the fabric of digital public culture in the same way that an event that is "newsworthy" merits public exposure and discussion even if it contains personal information and invades an individual's privacy. This section proposes newsworthiness as an arbiter of fairness for capitalizing

1. The distinction between public and private figures arises in the context of defamation and privacy litigation, especially First Amendment jurisprudence in the US. For the purposes of this article, non-public figures are persons whose actions and activities are subject to little or no *specific* public interest. See Susan M Gilles, "Public Plaintiffs and Private Facts: Should the 'Public Figure' Doctrine Be Transplanted into Privacy Law?" (2005) 83:4 Nebraska Law Review 1204. The usefulness of this distinction has also been considered as a way to align the right to be forgotten with the US First Amendment. See Michael L Rustad & Sanna Kulevska, "Reconceptualizing The Right to Be Forgotten to Enable Transatlantic Data Flow" (2015) 28:2 Harvard Journal of Law & Technology 349 at 354.
2. *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (13 May, 2014), Doc C-131/12, ECLI:EU:C:2014:317 (CJEU) [*Google Spain*]; EC, *Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31 [Directive 95/46/EC].

on popular user-generated content (though the term itself requires significant refinement), with the aim of allowing for digital public culture to flourish while still protecting privacy of data subjects. Part VI explores the attitude that publicly accessible information is "free for the taking", and how the US and Canada have placed restrictions on businesses that try to unfairly capitalize on this perception.

Overall, the following analysis will demonstrate that broader principles of information fairness should guide choices about how to protect data subjects from the far more powerful forces of commercial enterprises that deal in personal information products and services.

II. The EU's "Right to Be Forgotten" as a Restraint on Commercial Exploitation of Personal Information Online

The EU's implementation of the right to be forgotten is a good starting point for discussing information brokers, fairness, and privacy in publicly accessible personal information, because this right is centrally concerned with whether ongoing public access to personal information that has already been made available online should be permitted. There are two major versions of the right to be forgotten, neither of which is very well captured by the concept of "forgetting". The first is the right to obscurity, which is a narrow procedural remedy for data subjects operating within existing data protection obligations in the EU. The right to obscurity arises from the 2014 CJEU decision in *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzalez*,[3] which determined that data subjects have a right to require general search engines like Google to de-list certain links that appear in search results of their name, based on the characterization of search engines as information brokers.

The second is the right to erasure, which is a broader substantive right to require data controllers to erase certain online personal information;

3. *Google Spain*, *ibid.*

this will be implemented in the EU *General Data Protection Regulation*[4] ("*GDPR*") that comes into force in May 2018. This right to erasure applies to all data controllers including those that generate their own content (like news agencies), but when applied to secondary online information brokers (like search engines and hosts), it would mean ensuring that content does not appear in search results or otherwise on the hosting service, further reducing public accessibility of that information.[5] This article focuses on secondary information brokers that compile and present information garnered from other sources that do not originate with the business itself.

Two aspects of the *Google Spain* decision are particularly important to the following discussion: (1) the characterization of what Google does as information brokering — that is, the creation of a packaged profile of an individual, and (2) the determination that Google's activities are predominantly commercial rather than, for example, exercised in the public interest. A preliminary determination in *Google Spain* was based on whether Google and other general search engines are subject to the Data Protection Directive. The CJEU considered whether Google engaged in "processing" personal information as a "data controller" as set out in the Directive. The CJEU determined that it did, in that Google controls the algorithm that collects personal information from diverse online sources,

---

4. "[R]ight to be Forgotten, also known as Data Erasure, entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests". See "GDPR Key Changes" *EU General Data Protection Regulation*, online: EUGDPR <eugdpr.org/key-changes.html>.
5. For a fuller discussion of the contours of the right to be forgotten and how it might be implemented in Canada, see Andrea Slane, "Search Engines and the Right to Be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow"(forthcoming 2018) 55:2 Osgoode Hall Law Journal [Slane, "Squaring the Remedy"].

then collates and presents it to users in a ranked form.[6] When a person is searched by name, Google gathers available mentions across online sources and produces a profile that potentially has a greater impact on the privacy interests of the data subject than any one of those sources alone.[7]

As for the commercial nature of Google's activities, the CJEU focused on the most straightforward ways that Google makes money from searches, namely through its AdWords advertising program. AdWords uses a "pay per click" advertising model whereby advertisers bid for association with particular search terms, so that links to their sites come up at the top of search results, as tailored to the searcher's geographic area.[8] The CJEU wrote:

> [t]he very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory.[9]

The CJEU did not consider whether advertising appears on the same page of every type of search result, and whether this makes any difference to the overall analysis. In general, an individual's name, even a well-known public figure, does not serve as an AdWords linked keyword. However, if the individual's name is searched in conjunction with another term that is an AdWords keyword, then advertising links will appear. For example, if the complainant in the *Google Spain* case is searched in conjunction with the term "bankruptcy" (his complaint aimed to have Google de-list

---

6. *Google Spain*, *supra* note 2 at paras 32–33.
7. *Ibid* at para 37.
8. Rory Cellan-Jones, "How does Google make money?" *BBC News*, online: BBC iWonder <bbc.co.uk/guides/z9x6bk7>; Greg McFarlane, "How Does Google Make Its Money?" *Investopedia* (22 November 2012), online: Investopedia <investopedia.com/stock-analysis/2012/what-does-google-actually-make-money-from-goog1121.aspx>; Julia Love & Rishika Sadam, "Google parent Alphabet's profit up 29 percent on strong ad sales" *Reuters* (27 April 2017), online: Reuters <in.reuters.com/article/alphabet-results/google-parent-alphabets-profit-up-29-percent-on-strong-ad-sales-idINKBN17T2ZQ>.
9. *Google Spain*, *supra* note 2 at para 57.

links to public notices about past debt), then ads for debt relief services will appear at the top of the page.[10]

Nonetheless, having determined that Google is a "data controller" that "processes" personal information within an overall commercial business model that monetizes search results, the search engine is required, upon request, to remove links from the search results of a person's name where those links lead to information that is "inadequate, irrelevant, no longer relevant or excessive" to the purpose for which it was collected, unless there is a public interest in retaining the link to that information upon such a name search.[11]

For the most part, implementation of the *Google Spain* decision appears to be predominantly focused on results containing outdated personal information of non-public figures, where the privacy interests of the data subject outweigh the interests of the public in having access to that specific information through a search of that individual's name (such as a link revealing a long ago conviction for a minor crime).[12] It remains unclear whether the idea of "excessive to the purpose" could be meaningfully applied to a general search engine; if we characterize search engines' purpose for collection as providing a ranked compilation of *most* relevant publicly accessible online information related to that person, then "excessive" is a bit more refined than relevance alone. A search result could also be "excessive" if it returned highly sensitive information. Relevance and excessiveness must in any case be considered normative

---

10. "How Does Google Make Its Money: The 20 Most Expensive Keywords in Google AdWords" *Wordstream*, online: Wordstream <wordstream.com/articles/most-expensive-keywords>. This article used data from 2010–2011 and concluded that the most expensive pay per click word is "insurance" followed by "loans" and "mortgage".
11. The terms "inadequate, irrelevant, no longer relevant or excessive" come from the EU Data Protection Directive, Directive 95/46/EC, *supra* note 2, which requires at art 6(1)(c) that personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".
12. "Transparency Report: Search removals under European privacy law" *Google*, online: Google <transparencyreport.google.com/eu-privacy/overview> [Google Transparency Report].

terms, akin to "newsworthiness", which is similarly not dependent on the judgement of a particular individual reader, but rather defines the contours of legitimate public interest in having the information.[13]

Relevance and excessiveness relate to newsworthiness, in that relevance implies a public interest in access to this information that outweighs the data subject's privacy interests, an interest that is calculated via the sensitivity of the information at issue. Along these lines, data protection regimes typically exclude the practice of "journalism" from data protection obligations.[14] Therefore, the collection of personal information about the subject of a news item legitimately in the public's interest, even when carried out by a for-profit news organization, is not constrained by obligations that would restrict public access to that news item.[15] In passing, the CJEU rejected the possibility that what search engines do is journalism.[16] The Advocate General's opinion on the case offered some credence to the idea that search engines serve as archives, but reiterated European jurisprudence that has held that news archives

13. Newsworthiness is most often used in the US context in relation to defamation, right of publicity and publication of private facts cases. It has often been criticized by US scholars who consider it to permit too much encroachment on freedom of expression. See *e.g.* Amy Gajda, *The First Amendment Bubble: How Privacy and Paparazzi Threaten a Free Press* (Cambridge: Harvard University Press, 2015); Amy Gajda, "The Present of Newsworthiness" (2016) 50:2 New England Law Review 145. Others consider newsworthiness to provide too easy a justification for violating privacy. See Dianna M Worley, "*Shulman v Group W Productions*: Invasion of Privacy by Publication of Private Facts — Where Does California Draw the Line Between Newsworthy Information and Morbid Curiosity?" (2000) 27 Western State University Law Review 535 at 535.
14. In Canada, see *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 7(1)(c) [*PIPEDA*]. See also Teresa Scassa, "Journalistic Purposes and Private Sector Data Protection Legislation: Blogs, Tweets and Information Maps" (2010) 35:2 Queen's Law Journal 733.
15. For analysis of problems with determining where to draw the line regarding journalism versus commercial speech that can be more heavily regulated, see Diane Leenheer Zimmerman, "Who Put the Right in the Right of Publicity?" (1998) 9:1 DePaul-LCA Journal of Art and Entertainment Law and Policy 35 at 55.
16. *Google Spain*, *supra* note 2 at para 85.

have a greater duty to ensure accuracy of historical information, since the urgency of publishing current affairs is absent.[17] Alternatively, Google tried to claim that it cannot be a data controller because it does not distinguish between different types of data and does not alter that data in presenting results.[18] The CJEU rejected this argument, stating that it makes no difference that Google does not distinguish between personal data and other information, nor does it matter that "[t]hose data have already been published on the internet and are not altered by the search engine".[19]

Several scholars have strongly critiqued Google's assertion that its service merely delivers up informational history, and so serves as a form of cultural memory.[20] For example, Julia Powles noted that many online service providers have been capitalizing on the concept of the internet as a public sphere when really it is "[j]ust an algebraic representation of privately owned services".[21] She warned against equating this privately owned and manipulated network with our commitment to maintaining public records and archives offline (or even digitally stored, but subject to some access controls). In effect, Google is trying to have it both ways: to be legally recognized as the guardian of transparency in the online info-world, and yet, to conceal the algorithm by which such information

17. See *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (25 June, 2013), Doc C-131/12, ECLI:EU:C:2013:424 at para 123.
18. *Google Spain*, *supra* note 2 at para 22.
19. *Ibid* at paras 28–29.
20. For Google's position, see Richard S Whitt, "'Through a Glass, Darkly': Technical, Policy, and Financial Actions to Avert the Coming Digital Dark Ages" (2017) 33:2 Santa Clara High Technology Law Journal 117.
21. Julia Powles, "The Case That Won't Be Forgotten" (2015) 47:2 Loy University of Chicago Law Journal 583 at 591.

is retrieved and monetized.[22] Google claims to use more than 200 factors when compiling its ranking of search results, with popularity being a dominant factor. But even this one factor, as Powles notes, tends to exacerbate the "man bites dog" problem long recognized in journalism — that what is most popular and sells the most "papers" is not necessarily what is most current, accurate, or most central to overall historical records regarding an individual.[23]

The dominance of the popularity factor is further skewed by the demographics of the audience that most actively uses Google — which has historically been Western, white, middle-class men, although this is slowly changing.[24] The legacy of this bias is evident in studies that have revealed that Google searches are often skewed to favour privileged perspectives — delivering search results that positively reflect whites and negatively reflect African-Americans for instance (*e.g.* "beautiful dreadlocks" turns up images of white people while "unprofessional

22. Richard Curtis, "Google Wants It — and Has It — Both Ways" *Publishing in the 21st Century* (blog) (30 May 2012), online: Publishing in the 21st Century <curtisagency.com/blog/2012/05/google-wants-it-and-has-it-both-ways.html >; Uta Kohl, "Google: The Rise and Rise of Online Intermediaries in the Governance of the Internet and Beyond (Part 2)" (2013) 21:2 International Journal of Law and Information Technology 187 at 191–98.
23. Powles, *supra* note 21 at 610.
24. Bias in machine learning is common, because machines learn from humans and unfortunately humans are biased, especially online. See *e.g.* Aylin Caliskan, Joanna J Bryson & Arvind Narayanan, "Semantics derived automatically from language corpora contain human-like biases" (2017) 356:6334 Science, online: Science <science.sciencemag.org/content/356/6334/183.full>; Tolga Bolukbasi et al, "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings" (2016) arXiv 1607.06520v11, online: Cornell University Library <arxiv.org/pdf/1607.06520.pdf>.

hairstyles" brings up images of black people).[25] As Safiya Umoja Noble wrote:

> [i]t is dominant narratives about the objectivity and popularity of web search results that make misogynist or racist search results appear to be natural. Not only do they seem ["normal"] due to the technological blind spots of users who are unable to see the commercial interests operating in the background of search (deliberately obfuscated from their view), they also seem completely unavoidable because of the perceived ["popularity"] of sites as the factor that lifts websites to the top of the [results] pile.[26]

Further, Google has been called to task regarding how its AdWord algorithms work. One study found that searches of names associated with African-Americans were more likely to include ads for criminal record checks than neutral names or names associated with white people.[27] In other words, Google's business model delivers results and advertising skewed by existing social bias.

Google is constantly adjusting its algorithms and regularly attempts to address some of these concerns, but doing so merely reinforces the CJEU conclusion that Google indeed controls data collection, packaging, and presentation; Google search results are not neutral reflections of the material that is publicly available on the internet. Therefore, in terms of data protection and consumer protection, skewed results containing personal information should be addressed by requirements related to

25. Fiona Rutherford & Alan White, "This Is Why Some People Think Google's Results Are 'Racist'" *BuzzFeed* (12 April 2016), online: BuzzFeed <www.buzzfeed.com/fionarutherford/heres-why-some-people-think-googles-results-are-racist?utm_term=.kqpDg0ERB7#.dpKoZBwvqA>; Leigh Alexander, "Do Google's 'unprofessional hair' results show it is racist?" *The Guardian* (8 April 2016), online: The Guardian <theguardian.com/technology/2016/apr/08/does-google-unprofessional-hair-results-prove-algorithms-racist->.
26. Safiya Umoja Noble, "Google Search: Hyper-visibility as a Means of Rendering Black Women and Girls Invisible", (2013) 19 InVisible Culture, online: University of Rochester <ivc.lib.rochester.edu/google-search-hyper-visibility-as-a-means-of-rendering-black-women-and-girls-invisible/>.
27. Latanya Sweeney, "Discrimination in Online Ad Delivery" (2013) arXiv: 1301.6822 1, online: Cornell University Library <arxiv.org/pdf/1301.6822.pdf>.

relevance and excessiveness, more fairly balancing the interests of data subjects with the interests of searchers to easily find that information.

III. Using Fairness to Restrict Businesses that Facilitate Access to Public Documents Through Information Compilation Products

Since the advent of the internet, the easy accessibility of personal information has raised concerns about its use by the various gatekeepers of financial and professional opportunities — especially insurers, lenders, admissions officers, and potential employers.[28] Scholars and commentators have debated the best ways to address unfairness that can result from misuse of information found online — from legislation addressing the provision of the information, to legal restrictions on use, to ethical guidelines for these industries.[29] Parallel debates have focused on digitizing and facilitating public access to public documents, such as

28. "Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade" *CareerBuilder* (28 April 2016), online: CareerBuilder <careerbuilder.ca/share/aboutus/pressreleasesdetail.aspx?sd=4%2F28%2F2016&id=pr945&ed=12%2F31%2F2016>; Jonathan A Segal & Joyce LeMay, "POINT/COUNTERPOINT: Should Employers Use Social Media to Screen Job Applicants?" *HR Magazine* (1 November 2014), online: SHRM <www.shrm.org/hr-today/news/hr-magazine/pages/1114-social-media-screening.aspx>; Kaitlin Mulhere, "Lots More College Admissions Officers Are Checking Your Instagram and Facebook" *Money* (13 January 2016), online: Time <time.com/money/collection-post/4179392/college-applications-social-media/>; Stephanie Armour, "Borrowers Hit Social-Media Hurdles: Regulators Have Concerns About Lenders' Use of Facebook, Other Sites" *The Wall Street Journal* (8 January 2014), online: Wall Street Journal <www.wsj.com/articles/borrowers-hit-socialmedia-hurdles-1389224469>.

29. Avner Levin, "Losing the Battle but Winning the War: Why Online Information Should Be a Prohibited Ground" (2015) 18:2 Canadian Labour and Employment Law Journal 379; Nathan J Ebnet, "It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the *Fair Credit Reporting Act*" (2012–2013) 97:1 Minnesota Law Review 306.

court decisions and documents, or arrest and detention records.[30]

If Google qualifies as a "data controller" for the purposes of the EU Data Protection Directive, then surely other online businesses that specifically provide a compilation of material about an individual found in public records would also qualify. In the US, restrictions on such businesses are relatively limited, but the FTC has initiated investigations and issued rulings against some of these businesses, including under the *Fair Credit Reporting Act*[31] ("*FCRA*"). The text of the Act is promising in that it defines a "consumer report" as communication of any information by a consumer reporting agency:

> [b]earing on a consumer's credit worthiness … character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or [personal, family or household] insurance … (B) employment.[32]

The *FCRA* also sets out restrictions on specific information that should not be provided as part of a consumer credit report, including outdated financial information (generally after 7 years), bankruptcies after 10 years, arrest records (generally after 7 years), and "[a]ny other adverse item of information, other than records of conviction of crimes" (generally after 7 years).[33] These time limits are related in spirit to the EU's restriction on data controllers dealing in outdated and no longer relevant information,

---

30. Amanda Conley et al, "Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry" (2011–2012) 71:3 Maryland Law Review 772; Karen Eltis, "The Judicial System in the Digital Age: Revisiting the Relationship between Privacy and Accessibility in the Cyber Context" (2011) 56:2 McGill Law Journal 289.
31. In Canada, consumer reporting agencies are regulated by provincial legislation and require registration with a provincial authority. For instance, in Ontario, such agencies are governed by the *Consumer Reporting Act,* RSO 1990, c C-33. However, all businesses are subject to some form of data protection obligations, either the federal *PIPEDA* or substantially similar provincial legislation; for US, see *Fair Credit Reporting Act*, 15 USC § 1681a (1970) [*FCRA*].
32. *FCRA*, *ibid*, § 1681a(d)(1).
33. *Ibid*, § 1681c(a).

but the EU's definition of "data controller" is vastly broader than the *FCRA*'s definition of "consumer reporting agency".

The definition of a "consumer reporting agency" under the *FCRA* encompasses any person or organization that:

> [f]or monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.[34]

This definition is narrowed by the fact that "for the purpose of furnishing consumer reports" incorporates the definition of "consumer reports" as restricted to situations where the information collected is being provided "for the purpose of serving as a factor" in establishing creditworthiness or for employment purposes. The *FCRA* does not capture more general or unspecified purposes for collecting consumer information.

The consequences of this limitation are evident in the FTC's complaint brought forward by the US Attorney General against Spokeo in 2012.[35] Spokeo is an online service that assembles consumer information from online and offline sources to create "consumer profiles" to which it sells access to individuals or businesses. At the time of the complaint, Spokeo marketed its service specifically to the human resources industry as a background screening tool, offering high-volume access via subscription. After the court ruling against Spokeo for violating the *FCRA*, the end result has been that Spokeo no longer specifically markets its service to the human resources industry, but otherwise continues to operate its business in the same fashion, including by offering high-volume subscriptions.[36]

Since the Spokeo ruling, other personal information compilation services have also merely posted disclaimers that their services should not be used for *FCRA*-covered purposes. Truthfinder.com, for instance,

---

34. *Ibid*, § 1681a(f).
35. US, Federal Trade Commission, *United States v Spokeo Inc* (CV12-05001) (2012).
36. Spokeo instead claims that high volume subscriptions "generally appeal to professionals whose work routine includes constant people research". See "FAQs: what are quota upgrades?" *Spokeo*, online: Spokeo <www.spokeo.com/faqs-consumer>.

requires users to click an "I understand" button to enter the site, affirming consent to the statement that:

> TruthFinder does not provide consumer reports and is not a consumer reporting agency. We provide a lot of sensitive information that can be used to satisfy your curiosity, protect your family, and find the truth about the people in your life. You may not use our service or the information it provides to make decisions about consumer credit, employers, insurance, tenant screening, or any other purposes that would require [*FCRA*] compliance.[37]

Instead, Truthfinder's marketing is primarily aimed at individuals who want to learn "the truth about the history of your family and friends", although the service offers "Power Users" a discount for purchasing three months of unlimited searching.[38] Another *FCRA* disclaimer appears in tiny print at the bottom of the welcome page, stating:

> [t]he information available on our website may not be 100% accurate, complete, or up to date, so do not use it as a substitute for your own due diligence, especially if you have concerns about a person's criminal history. TruthFinder does not make any representation or warranty about the accuracy of the information available through our website or about the character or integrity of the person about whom you inquire.[39]

Truthfinder thus does not take any responsibility for the accuracy of its contents, despite what is implied in its name and marketing.

A very similar *FCRA* disclaimer appears on commercial mugshot and arrest record websites, which offer a way to acquire a compilation of this subset of public records, generally scraped from law enforcement and detention centre websites that make such information available online to the public.[40] Debates about the value and purpose of making these sorts of pre-conviction and non-conviction documents a matter of public record have included the public interest argument that publicly inspectable records help ensure the transparency and fairness of the criminal justice system.[41] However, making such records easy to acquire feeds more into

37. *Truthfinder*, online: Truthfinder <www.truthfinder.com>.
38. *Ibid*.
39. *Ibid*.
40. See *e.g. Mugshots*, online: Mugshots <www.mugshots.com> [Mugshots].
41. Danielle Bruno, "Note: Mugshots Or Public Interest? Why FOIA Exemption 7(C) Does Not Categorically Exempt Booking Photographs from Disclosure" (2016) 78 University of Pittsburgh Law Review 95.

the socially punitive approach to persons in conflict with the law. From this perspective, easy-to-access mugshots and arrest records not only allow people to protect themselves from these individuals, but also heighten the effects of conflict with the law through public shaming, even when an individual has not been convicted of a crime. Some US states and counties have made arrest and detention records publicly available online, while others are more restrictive in their release of this information.[42] Publicly available law enforcement and jail websites generally include disclaimers warning that errors and inaccuracies in the information provided are common, and reiterating the basic criminal justice tenet of innocence until proven guilty.[43] EU and Canadian law enforcement organizations generally do not make such information freely available online.[44]

Commercial mugshot and arrest record websites feature similar disclaimers to law enforcement and jail sites.[45] However, commercial sites tend to retain mugshot, arrest, and detention records indefinitely, still

---

42. Martin A Holland, "Note: Identity, Privacy and Crime: Privacy and Public Records in Florida" (2012) 23 University of Florida Journal of Law & Public Policy 235.
43. For instance, see "Johnson County Iowa Jail Roster Disclaimer" *Johnson County Iowa*, online: Johnson County Iowa <www.johnson-county.com/Sheriff/JailRoster/Index> [Johnson County Iowa].
44. In Canada, public disclosure of personal information by the government without the individual's consent is generally prohibited by *Privacy Act*, RSC 1985, c P-21, s 8.
45. Mugshots.com prominently displays such a disclaimer, including (in ALL CAPS) that "[T]HE MUGSHOTS AND/OR ARREST RECORDS PUBLISHED ON MUGSHOTS.COM ARE IN NO WAY AN INDICATION OF GUILT AND THEY ARE NOT EVIDENCE THAT AN ACTUAL CRIME HAS BEEN COMMITTED. ARREST DOES NOT IMPLY GUILT, AND CRIMINAL CHARGES ARE MERELY ACCUSATIONS. A DEFENDANT IS PRESUMED INNOCENT UNLESS PROVEN GUILTY AND CONVICTED. FOR LATEST CASE STATUS, CONTACT THE OFFICIAL LAW ENFORCEMENT AGENCY WHICH ORIGINALLY RELEASED THE INFORMATION". See Mugshots, *supra* note 40.

without updating or correcting incorrect information.[46] For example, Mugshots.com, the most prominent of these sites, calls itself a "Google for Mugshots", states the following:

> [t]he website is a search engine for Official Law Enforcement records, specifically booking photographs, mugshots. Originally collected and distributed by Law Enforcement agencies, booking records are considered and legally recognized as public records, in the public domain. Mugshots.com republishes these Official Records in their original form ("as is") under the First Amendment to the United States Constitution, the freedom to publish true and factual information. Our intent is to provide a legitimate and useful service for both the private and public sectors.[47]

The site recognizes no irony in the disconnect between characterizing the First Amendment as guaranteeing "the freedom to publish true and factual information" and a disclaimer denying responsibility for accuracy. In response to the questions "[m]y record was expunged"; "[I] was pardoned"; "[m]y case was dismissed"; and "[w]ill you remove my mugshot?", the Mugshots.com FAQ page states, "[a]s you may be aware [e]xpungement and pardon only apply to certain government agencies' databases, and not all of them. Certainly not to the private sector".[48] In other words, according to Mugshots.com, whatever balancing the public sector engages in to justify granting a pardon or expungement does not apply to public records that are archived by private entities.

Sites like Mugshots.com capitalize on US First Amendment jurisprudence, which permits further dissemination of truthful

---

46. The duration which arrest records are kept by public offices in US states varies. The Hillsborough County Florida Sheriff's Office posts the following notice: "Arrest information is a Public Record under Florida State Law unless it has been ordered sealed or expunged. Online arrest inquiries are available for adult arrests occurring since January 1, 1995 for which the Hillsborough County Sheriff's Office has an electronic record". See "Arrest Inquiry" *Hillsborough County Sheriff's Office*, online: HCSO <webapps.hcso.tampa.fl.us/ArrestInquiry#>. The Johnson County Iowa Jail Roster only contains names of individuals who are or have been held by the Johnson County Sheriff within the last 48 hours. See Johnson County Iowa, *supra* note 43.
47. "About" *Mugshots*, online: Mugshots <mugshots.com/about.html>.
48. "FAQ" *Mugshots*, online: Mugshots <mugshots.com/faq.html>.

information if it was released by its original custodian, even if the release itself was against the law or public policy.[49] Thus, even if the original source cannot vouch for the accuracy of the information, mugshot websites in the US are currently under no obligation to update inaccurate or outdated information, even in the face of a direct complaint. However, even in the US, commercial mugshot and arrest record websites have come under fire for using a business model whereby individuals can pay a fee to have their profile removed, altered, or updated, prompting some US states to enact legislation that prohibits the use of public records in this sort of business model, especially where the person has not been convicted.[50] Most states do not prohibit it, so Mugshots.com, until at least September 2017, continued to offer "content removal services" through UnpublishArrest.com, which it bills as its exclusive "licensee" to specifically handle removal and editing requests to Mugshots.com. In May 2018, the state of California charged four proprietors of Mugshots.com with extortion, money laundering, and identity theft in relation to this fee-for-removal scheme, and as of this writing the site now simply refuses to remove content at all, standing on the claim to be entitled to

49. *Florida Star v BJF*, 491 US 524 (1989) [*Florida Star*].

50. "Mug Shots and Booking Photo Websites" *National Conference of State Legislatures* (23 October 2017), online: NCSL <ncsl.org/research/telecommunications-and-information-technology/mug-shots-and-booking-photo-websites.aspx>; Bruno, *supra* note 41; Sean P Sullivan, "Mugshot 'extortion' website ban signed by Christie" *NJ.com* (23 July 2017), online: NJ.com <nj.com/politics/index.ssf/2017/07/christie_signs_bill_banning_mugshot_extortion.html>; David Harris, "New law forces websites to pull mug shots of the acquitted" *Orlando Sentinel* (19 June 2017), online: Orlando Sentinel <orlandosentinel.com/news/breaking-news/os-public-records-mugshots-florida-20170619-story.html>.

republish information issued by law enforcement agencies "as is".[51]

In addition to the fee structure, the overarching business model for a site like Mugshots.com is advertising driven. The dynamics of the ads it runs capitalize on both sides of the online personal information market. On one hand, there are prominent ads for Cleansearch.net, which offers to remove results from general search engines and so targets data subjects. On the other hand, there are ads to fee-charging profile compilation services — mostly via search boxes that look like they are merely additional internal search engines to Mugshots.com, but actually bring the searcher to an external site — and so target data seekers. Links lead searchers to BeenVerified.com (which often uses the slogan "This Site's Deep Search Can Reveal More Than Google"), Peoplelooker.com, Instantcheckmate.com, and Truthfinder.com — all of which offer personal information profile compilation for a fee, either per report or as a monthly subscription.[52] Mugshots.com also employs Google AdSense, which delivers sidebar ads tailored to the search history of individual users, regardless of the content of the website.

In 2013, in response to criticism of the business practices of commercial mugshot websites like Mugshots.com, Google implemented a voluntary change to its algorithm to demote name search results linking to such sites; they are not de-listed entirely, but appear lower on the

---

51. Until the scheme was dismantled in late 2017, mugshots.com charged USD$399 to remove, permanently publish, or edit one arrest record. See e.g. *Internet Archive: Wayback Machine* (27 September 2017), online: Internet Archive: Wayback Machine <https://web.archive.org/web/20170927005616/http://unpublisharrest.com/>; *Internet Archive: Wayback Machine* (3 November 2017), online: Internet Archive: Wayback Machine <https://web.archive.org/web/20171103230426/https://chase44.wufoo.com/forms/zr7v2lm1svib3r/>; Cyrus Farivar, "All of Mugshots.com's alleged co-owners arrested on extortion charges" *Ars Technica* (17 May 2018), online: Ars Technica <https://arstechnica.com/tech-policy/2018/05/all-of-mugshots-coms-alleged-co-owners-arrested-on-extortion-charges>; "FAQ" *Mugshots*, *supra* note 48.

52. One-month subscriptions tend to hover just under USD $30. See for instance *Truthfinder*, online: Truthfinder <https://www.truthfinder.help/cost/>.

results list.[53] Searchers are free to choose to go directly to the site and partake in the service and its economy directly, but Google has chosen to make it more difficult for a searcher who is not specifically looking for this sort of information to inadvertently find it. The fix is not foolproof however. For example, using Google to search the uniquely spelled name of a woman whose image is posted on the non-consensual pornography website MyEx.com, along with her state of residence, produces a results list prominently containing links to multiple sites detailing her arrest record, including both law enforcement institutions and Mugshots.com. Further, as noted above, if a person's name is entered followed by the search term "arrest", not only are these sites likely to rise to the top, but the results will include paid AdWords links to commercial public records compilation services like Truthfinder.com.

The public policy commitments related to public access to pre-conviction and non-conviction information, as well as criminal conviction records, vary significantly by jurisdiction, in ways that profoundly shape this market for sensitive personal information.[54] Many scholars have noted the influence of a longer tradition of personality rights protection in continental Europe, which is widely considered to be the backdrop for the current embrace of "the right to be forgotten". Apart from not providing public access to past criminal conviction records, some European countries even forbid public discussion of past criminal convictions by media organizations, including documentary filmmakers attempting to explore historical crimes.[55] In Canada, criminal convictions, pre-conviction status, and non-conviction records are not

53. Barry Schwartz, "Google Launches Fix to Stop Mugshot Sites from Ranking: Google's MugShot Algorithm" *Search Engine Land* (7 October 2013), online: Search Engine Land <searchengineland.com/google-launches-fix-to-stop-mugshot-sites-from-ranking-googles-mugshot-algorithm-173672>.

54. James B Jacobs, *The Eternal Criminal Record* (Cambridge: Harvard University Press, 2015).

55. See discussion of European approach in Franz Werro, "The Right to Inform v the Right to Be Forgotten: A Transatlantic Clash" in Aurelia Colombi Ciacchi et al, eds, *Liability in the Third Millennium* (Baden-Baden: Nomos, 2009) 285 at 290.

freely open to the public; they are housed in a law enforcement database — Canadian Police Information Centre ("CPIC") — and are only made available upon legitimate request, usually with the consent of the data subject (for instance, when a person wants to volunteer in a school). The rationale for these restrictions is based on the principle that such personal information is always sensitive, that ongoing public disclosure is highly likely to negatively affect the individual, and that the inability to shield this information from ongoing public disclosure damages the individual's chances of rehabilitation and reintegration.[56]

Further, Canada makes "record suspensions" available to eligible individuals who apply for them, similar to European jurisdictions, although unlike some European countries, Canada does not prevent the reporting or republishing of information about past crimes. A record suspension (formerly referred to as a pardon) removes a criminal conviction record from the parts of the CPIC database that are available to the public upon legitimate request.[57] Access to the full record is

56. Jeannie Stiglic, "Hard to check criminal records of others: Only legal way is through court documents" *CBC News* (13 January 2012), online: CBC <cbc.ca/news/canada/hard-to-check-criminal-records-of-others-1.1145038>. This is not to say that injustices do not continue to be perpetuated against people who have been in conflict with the law, since many potential employers require police record checks without much justification other than prejudice. See Canadian Civil Liberties Association, "False Promises, Hidden Costs: The Case for Reframing Employment and Volunteer Police Record Check Practices in Canada", by Abby Deshman (Toronto: CCLA, May 2014), online: CCLA <ccla.org/recordchecks/falsepromises>. See also Canadian Civil Liberties Association, "Presumption of Guilt? The Disclosure of Non-Conviction Records in Police Background Checks", by Graeme Norton (Toronto: CCLA, May 2012), online: CCLA <ccla.org/cclanewsite/wp-content/uploads/2015/02/Presumption-of-Guilt.pdf>.

57. Convictions for which a record suspension has been granted may still be released pursuant to a Police Vulnerable Sector Check, which is sought by people seeking employment or volunteering in a position of authority or trust relative to vulnerable persons. For instance, see Ontario Provincial Police, "Criminal Record Checks and Police Checks" (OPP, 26 October 2017), online: OPP <opp.ca/index.php?id=115&entryid=56a1276d8f94acdb5824a3d7>.

retained by police, and public accessibility according to the above noted restrictions can be reinstated if the individual commits another offence.[58] Overall, the US is far less generous in its protection of people with criminal records, and pardons are much more rare — there are some other administrative means of providing limited relief from the burden of having a criminal record, but none of them affect previous, existing, or future publication of the fact of conviction.[59]

The key issue here is ease of access versus obscurity, or put more materially, public accessibility to conviction records upon legitimate request versus accessibility by mere payment of a fee. Further, websites that provide public records can choose whether to allow their contents to be crawled and indexed by general search engines like Google. Most court and tribunal websites, as well as legal information repositories like the various Legal Information Institute sites, offer internal search tools but opt not to permit external search engines to index their content. In Canada, the Office of the Privacy Commissioner ("OPC") ruled complaints against Globe24h, a website based in Romania, to be well-founded.[60] The website had scraped content from Canadian legal information sites, including CanLII, and allowed the reposted court and tribunal documents to be searched by external search engines.[61] One aspect of the Globe24h business model was to charge a fee to individuals

58. For Canada, see Royal Canadian Mounted Police, "Dissemination of Criminal Record Information policy", (RCMP, 24 June 2014), online: RCMP <rcmp-grc.gc.ca/en/dissemination-criminal-record-information-policy>.

59. *Collateral Consequences Resource Center: Collateral Consequence of Criminal Conviction and Restoration of Rights: News, Commentary, and Tools*, online: CCRC <ccresourcecenter.org>; Peter Leasure & Tia Stevens Andersen, "The Effectiveness of Certificates of Relief as Collateral Consequence Relief Mechanisms: An Experimental Study" (2016) 35 Yale Law & Policy Review Inter Alia 11, online: Yale University <www.ylpr.yale.edu/sites/default/files/IA/leasure.certificates_of_relief.produced.pdf>.

60. Office of the Privacy Commissioner of Canada, *Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA*, *PIPEDA* Report of Findings #2015-002 (Ottawa: OPC, 5 June 2015).

61. *Ibid*.

wishing to have their personal information removed from the site, as well as employing advertising. Globe24h claimed the documents were in the public domain and that it was free to repost the material and to make it more easily accessible to searchers, and refused to comply with the OPC's finding.

One complainant, joined by the OPC, brought the case to the Federal Court, which affirmed the findings of the OPC and held that Globe24h was disrupting the balancing done by courts, tribunals, and publicly accessible legal databases like CanLII, between the open court principle and the privacy interests of people whose personal information appears in these documents.[62] The Court ruled that making court documents searchable by general search engines does not further the interests of the open-court principle that justifies courts and tribunals making information public. Consequently, Globe24h is required to obtain the consent of data subjects in order to republish decisions and documents and make them externally searchable. The Court endorsed the OPC's support of a corrective court order requiring Globe24h to remove Canadian cases containing personal information, to take steps to remove these decisions from search engine caches, and to take steps to ensure that any documents reposted were not indexed by search engines. The Court also granted a declaratory order that the complainant can then take to Google per its voluntary removal policy for court orders. Unlike the CJEU, the Canadian Court was not asked to determine whether general search engines like Google would be required to de-index links to this material coming up in a name search for a data subject.

Globe24h argued that it should qualify for either the journalistic purpose or the publicly available information exemptions to application of Canada's private sector data protection legislation, the *Personal Information Protection and Electronic Documents Act*[63] ("*PIPEDA*"). The Court ruled that Globe24h was not engaging in a journalistic purpose when it republished court and tribunal documents and allowed them to be indexed by search engines, relying on the Canadian Association

62. *AT v Globe24h.com*, 2017 FC 114.

63. *Ibid* at para 29, referring to *PIPEDA*, *supra* note 14.

of Journalists' definition as suggested by the OPC. According to that definition, an activity qualifies as journalism only when: (1) its purpose is to inform the community on issues the community is interested in; (2) the presentation of the information involves an element of original production; and (3) it incorporates a "[s]elf-conscious discipline calculated to provide an accurate and fair description of facts, opinion and debate at play within a situation".[64] Thus, fairness once again provides a core measure for whether personal information is being made more easily publicly accessible in the public interest. The Court also rejected the defendant's efforts to use the "publicly available" exemption, stating the exemption only applies if the defendant's collection, use, or disclosure relates directly to the purpose for which the information appears in the public record or the original source. Again, court and tribunal records or documents are only exempt from further obligations if their republication furthers the open-court principle.[65]

This ruling suggests that general search engines like Google would also potentially be subject to *PIPEDA* in Canada, in that its search results that contain personal information would similarly not meet the criteria for either of these exemptions, though the OPC has not yet taken this stance.[66]

---

64. *Ibid* at para 68.
65. *Ibid* at para 78.
66. In *Google Inc v Equustek Solutions Inc*, the Supreme Court of Canada upheld an interlocutory injunction of worldwide reach against Google, requiring it to de-list the defendant's websites that sold wares in violation of plaintiff's intellectual property rights. The court rejected Google's claim that such an injunction interferes with freedom of expression and international comity, stating that there was no evidence on the record that any jurisdiction across the world would view the particular speech at issue as protected speech (that is, speech aiming to pass off the wares of the plaintiff as the defendant's). Google could apply for a variance if it was able to prove that protected speech was at issue. The case suggests that where there is variance between jurisdictions, that de-listing should be limited geographically to those jurisdictions where de-listing is considered a justified restriction on freedom of expression. See *Google Inc v Equustek Solutions Inc*, 2017 SCC 34 at paras 46–48.

IV. Businesses that Facilitate and Package User-Generated Content

The second major category of material that is to varying degrees public, or more accurately publicly accessible, is user-generated content. This may appear on social networking platforms or through websites serving as a forum for user-posted material. Indeed, Google reports that most of the top 10 sites for which it receives de-listing requests after the CJEU ruling are sites that host user-provided content.[67] The regulation of sites and services that host user-posted content has been controversial, given the widely recognized policy of immunizing hosts from liability for third-party-provided content. The degree of immunity varies by jurisdiction; the EU provides hosts immunity from liability for user-posted content but revokes that immunity if the host does not respond promptly to notice of illegal content, whereas the US provides broad immunity through the *Communications Decency Act*[68] ("*CDA*"), section 230, which imposes no obligation on hosts to respond to complaints about user-posted material. Whether general information location services like Google could (or should) be considered mere hosts or intermediaries of third-party content that turn up in search results, and hence be wholly or partially sheltered from liability, is an open question and would likely be answered differently by the US and EU, with Canada undecided.[69]

The US has struggled with host immunity in its efforts to curtail businesses that specifically profit from user-generated content in the category of non-consensual pornography ("revenge porn") — that is, sites that encourage users to post intimate images for public consumption

67. Google Transparency Report, *supra* note 12. The top 10 sites include social media juggernauts Facebook, YouTube, Twitter, and Instagram (last visited on 5 June 2017).

68. EC, *Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*, [2000] OJ L 178/1, art 14, online: EUR-Lex <eur-lex.europa.eu/eli/dir/2000/31/oj> [Directive 2000/31/EC]; *Communications Decency Act*, 47 USC § 230 [*CDA*], is the common name for Title V of the *Telecommunications Act* of *1996*.

69. Slane, "Squaring the Remedy", *supra* note 5.

without the consent of the person pictured. While many jurisdictions have now created criminal offences that prohibit posting such images without consent, for the most part these offences do not apply to the host or platform that houses them or else are not enforced against such hosts.[70] In the US, with the exception of host sites whose operators have been found guilty of other offences (*e.g.* hacking, identity theft, or extortion), the operators of online businesses that exploit the criminal acts of users have so far generally been assumed to be sheltered by *CDA*, section 230.[71]

To date, only one site has been investigated and ruled against by the FTC, which found that defendant Craig Brittain, who operated the site IsAnybodyDown, had:

> [u]nfairly disseminated photographs of individuals with their intimate parts exposed, along with personal information about them, for commercial gain and without the knowledge or consent of those depicted, despite the fact that he knew or should have known that the individuals had a reasonable expectation that their image would not be disseminated in that manner.[72]

What the FTC means by "in that manner" is dissemination on commercial or for-profit pornography websites, ordering that Brittain must remove all photos for which he did not have proof of consent and going forward, he must secure proof of consent of the person pictured before allowing a user to post that person's intimate image.[73]

Brittain, like the website operators convicted of criminal offences, also engaged in further unfair and deceptive business practices, such as tricking women into sending him intimate photos by posing as another woman on Craigslist, operating a "bounty system" to facilitate posting of specific people's images, and a fee-for-removal model. Nonetheless, the

---

70. Andrea Slane & Ganaele Langlois, "Debunking the Myth of Not My Bad: Sexual Images, Consent, and Online Host Responsibilities in Canada" (2018) 30:1 Canadian Journal of Women and the Law 42 [Slane & Langlois, "Debunking the Myth"].
71. *CDA*, *supra* note 68.
72. US, Federal Trade Commission, *Analysis of Proposed Consent Order to Aid Public Comment: In the Matter of Craig Brittain*, File No 132 3120, (FTC, 29 January 2015), online: FTC <https://www.ftc.gov/system/files/documents/cases/150129craigbrittainanalysis.pdf>.
73. Slane & Langlois, "Debunking the Myth", *supra* note 70.

FTC includes the more common and not as obviously unfair practice of soliciting users to post intimate images of other people without ensuring consent in its list of unfair business practices.[74] However, this kind of practice continued to be used by other non-consensual pornography sites, despite the FTC ruling against Brittain. For example, the still-operational website MyEx.com, operational until January 2018 when it went offline as part of a settlement with the FTC, invited users to post images of their former lovers, along with identifying information, and disavowed any obligation to ensure users had the photo subject's consent. MyEx.com monetized traffic to and from the site in various ways: in addition to the general Google Analytics tracking tool, MyEx.com employed Advertising.com (a tracker that matches ads with the content and types of users of a website), EroAdvertising (a more specialized targeted advertising tracker for porn-related advertising), and Adult Webmaster Empire (an affiliate program, whereby websites like MyEx.com are compensated for driving traffic onto a range of other commercial porn websites).[75]

In the US, websites like MyEx.com, like other websites that host third-party content, have assumed they are immune from any responsibility regarding material posted by users, under section 230 of the *CDA*. However, this immunity is based on the assumption that such websites are not serving as data controllers that process the personal information of consumers (albeit non-users of the service) when they provide a specific hosting service like this one. Following *Google Spain*, it is clear that the EU takes a different approach, considering business models to be processing personal information even when they are simply compiling and packaging information posted by others.[76] The EU data protection requirements are supplemented by the conditional immunity

74. US, Federal Trade Commission, *In the Matter of Craig Brittain: Complaint* (C-4564) (2016) at para 5.

75. Ganaele Langlois & Andrea Slane, "Economies of Reputation: The Case of Revenge Porn" (2017) 14:2 Communication & Critical/Cultural Studies 120; *US Federal Trade Commission and State of Nevada v EMP Media Inc, et al*, Stipulated Order for Permanent Injuction on Monetary (2018) 2:18-cv-00035 at 5-6.

76. *Google Spain*, *supra* note 2 at para 29.

provided to hosts by the EU E-Commerce Directive, which requires businesses to take down illegal material posted by third parties upon notification.[77] It is unlikely that a non-consensual pornography business would be able to comply with data protection requirements in the EU at all, but at the very least this kind of business would be required to take non-consensually posted intimate material down without charging a fee.

Canada has not formally applied its private-sector data protection regime to non-consensual pornography-hosting websites, although the OPC does claim to have successfully advocated on behalf of complainants to have images taken down.[78] In other online contexts, the OPC has several times imposed data protection obligations on a service provider that allows users to post or otherwise offer up a non-user's personal information; for example, in 2009, the OPC found Facebook to have violated *PIPEDA* with regard to a feature that prompted users to provide the email addresses of people they know who were not yet users of Facebook.[79] The OPC found that there should be "[a] clear distinction between activities conducted by Facebook users for strictly personal reasons and activities in which Facebook itself is involved".[80] To illustrate, the OPC continued:

> [w]hen users post information about non-users to their profiles, Walls, or News Feeds, such postings are made for personal purposes and as such fall outside the purview of the Act. The Act would apply only where Facebook uses non-users'

77. Directive 2000/31/EC, *supra* note 68.
78. Office of the Privacy Commissioner of Canada, "Online Reputation: What are they saying about me?" (Ottawa: OPC, 21 January 2016), online: OPC <priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/> [OPC, "Online Reputation"].
79. Office of the Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPIC) Against Facebook Inc Under the Personal Information Protection and Electronic Documents Act*, by Elizabeth Denham, *PIPEDA* Report of Findings #2009-008 (Ottawa: OPC, 16 July 2009) [Denham]. See also Office of the Privacy Commissioner of Canada, "Facebook investigation follow-up complete" (Ottawa: OPC, 22 September 2010), online: OPC <priv.gc.ca/en/opc-news/news-and-announcements/2010/bg_100922/>.
80. Denham, *ibid* at para 306.

> personal information for purposes of its own.[81]

Determination of when a business is using non-user personal information "for purposes of its own" within a business model based on advertising, traffic direction, and close ties to information removal services also varies by jurisdiction; Canada must choose between the approaches used in the EU and the US. The business model of non-consensual pornography websites — *i.e.* solicitation and monetization of sensitive personal information of non-users — should count as using personal information for the business's own purposes. By this logic, the OPC could also consider, as the CJEU did, that search engines like Google specifically profit from search results, although profiting from search of a person's name is less clear.

What is clear is that the OPC considers indexing by search engines to increase the effects of privacy concerns about information posted online, whether that information is public documents as in the Globe24h case described above, or is posted by users. In a 2012 finding against the Canadian youth-oriented social networking site, Nexopia, the OPC found that allowing user profiles and all their contents to be indexed by search engines as a default setting was not within the scope of what a reasonable person would expect from a social networking site, even if, as Nexopia argued, it markets itself as a more outward-facing, public exposure-oriented alternative to Facebook.[82] The OPC recommended that "visible to friends" should be the default privacy setting, and to make it obvious and explicit that choosing "visible to all" would include indexing via external search engines.[83]

While the EU, the US, and Canada clearly use different approaches, all three jurisdictions distinguish between businesses that merely host third-party content, and businesses that assist in creating content that uses personal information of users or non-users as part of its profit-

---

81. *Ibid*.
82. Office of the Privacy Commissioner of Canada, *Social networking site for youth, Nexopia, breached Canadian privacy law*, *PIPEDA* Report of Findings #2012-001 (Ottawa: OPC, 18 February 2013) at para 71.
83. *Ibid* at para 107.

making activity.[84] In response to public pressure to curtail the effects of non-consensual pornography businesses on victims, many mainstream US-based companies have voluntarily chosen to make it easier for these data subjects to successfully request removal of intimate images they did not consent to have publicly posted, including Reddit, Facebook, Twitter, Microsoft, and Google.[85] Facebook recently announced it would employ a photo identification system to block the reposting of such images it

84. *Fair Housing Council of San Fernando Valley v Roommates.com, LLC*, 521 F (3d) 1157 (9th Cir 2008) (US); Mary Anne Franks, "The Lawless Internet? Myths and Misconceptions About CDA Section 230", *Huff Post* (blog) (18 December 2013), online: Huffington Post <huffingtonpost.com/mary-anne-franks/section-230-the-lawless-internet_b_4455090.html>.

85. All of these services announced new policies in 2015 regarding take-down of intimate images housed on their services upon complaint by the victim. Andrea Peterson, "Reddit is finally cracking down on revenge porn" *The Washington Post* (24 February 2015), online: Washington Post <washingtonpost.com/news/the-switch/wp/2015/02/24/reddit-is-finally-cracking-down-on-revenge-porn/?utm_term=.df3926415b93>; Hayley Tsukayama, "Twitter updates its rules to specifically ban 'revenge porn'" *The Washington Post* (11 March 2015), online: Washington Post <www.washingtonpost.com/news/the-switch/wp/2015/03/11/twitter-updates-its-rules-to-specifically-ban-revenge-porn/?utm_term=.46ee8ea4384f>; Vindu Goel, "Facebook Clarifies Rules on What It Bans and Why" *New York Times: Bits* (blog) (16 March 2015), online: NY Times <bits.blogs.nytimes.com/2015/03/16/facebook-explains-what-it-bans-and-why/?mcubz=0>; Alyssa Newcomb, "How Microsoft Is Waging War Against Revenge Porn" *ABC News* (23 July 2015), online: ABC <abcnews.go.com/Technology/microsoft-waging-war-revenge-porn/story?id=32639751>; Jeff John Roberts, "Google to remove 'revenge porn' links at victims' request" *Fortune* (19 June 2015), online: Fortune <fortune.com/2015/06/19/google-revenge-porn-removal/>.

had already taken down.[86] In the US, these are voluntary policies and are limited to non-consensual pornography, nonetheless these voluntary policies are efforts to distinguish ethical platforms from unethical ones, where the former engage in striking a normatively fair balance between their incentives to make information easily accessible and the interests of people whose personal information is circulating.

Harnessing privacy invasion for profit via the attention economy drives many online business models. If this economy is to be fair, then an appropriate balance is needed between competing stakeholder interests, a balance that considers the sensitivity of the information (often correlated with harm or risk of harm to the data subject), and the public interest in easy access to that information.

V. Viral Content: When Online Personal Information Becomes Part of Public Culture

The public interest in access to content that includes the personal information of others is malleable, especially in an online context where viral distribution of some online material may render it a part of public culture. However, here too balancing of interests — by way of an analysis akin to newsworthiness — can help determine whether virality is sufficient to justify ongoing easy access to that content.

In the attention economy, the "subculture of humiliation" ensures

86. Matt Burgess, "Facebook is using photo-matching to tackle 'revenge porn'" *Wired* (6 April 2017), online: Wired <wired.co.uk/article/facebook-revenge-porn-tools>. In the Facebook Moderation Guidelines leaked to the press in May 2017, the internal Facebook document stated that Facebook had flagged more than 50,000 posts as related to non-consensual intimate imagery and sextortion in the month of January 2017 alone. The guidelines set out an escalation and removal protocol. See Nick Hopkins, "Revealed: Facebook's internal rulebook on sex, terrorism and violence" *The Guardian* (21 May 2017), online: The Guardian <www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence>; see especially "What Facebook says on sextortion and revenge porn" *The Guardian* (22 May 2017), online: The Guardian <www.theguardian.com/news/gallery/2017/may/22/what-facebook-says-on-sextortion-and-revenge-porn>.

that public circulation of sensitive personal information can be especially profitable for online businesses. For example, consider materials that mock or otherwise harass a person with disabilities. One of the earliest and most controversial cases of this sort involved an Italian court's conviction of three Google executives for criminal privacy invasion in 2010, charges that arose from users posting a video of an autistic boy being physically bullied to Google Video (its video-sharing platform prior to its purchase of YouTube).[87] The decision was widely criticized as misconstruing service provider obligations both in the US and in Europe, and the decision was overturned by an Italian appellate court in 2012. The Court of Appeals found that Google served as a host and had no obligation to monitor user postings, and had responded promptly by removing the video once expressly notified.[88]

While not discussed in the case, had Google not removed the video upon being notified, it likely would have been liable for the criminal offences charged, and also subject to data protection obligations related to the sensitive personal information of the autistic boy pictured in the video. Following *Google Spain*, Google would have been found to be a "data controller" profiting from the exploitation of this video; in the two months in which it was publicly available, Google Video algorithms had ranked the video highly in the "funny video" category and the Google AdWords service had automatically associated specific search terms with the video.[89] In other words, Google collected profits from the public

87. Manuela D'Alessandro, "Google executives convicted for Italy autism video" *Reuters* (24 February 2010), online: Reuters <www.reuters.com/article/us-italy-google-conviction-idUSTRE61N2G520100224>; Ernesto Apa & Oreste Pollicino, *Modeling the Liability of Internet Service Providers: Google vs Vivi Down, A Constitutional Perspective* (Milan: Egea, 2013).

88. "Court of appeals overturns conviction of Google Italy executives, redefines liability of hosting providers under privacy legislation" *Lexology* (26 March 2013), online: Lexology <www.lexology.com/library/detail.aspx?g=b36ffdc4-ee2b-4dfb-ae83-01bcb15ff5f7>.

89. Bruno Carotti, "The *Google — Vivi Down* Case: Providers' Responsibility, Privacy and Internet Freedom" in Sabino Cassese et al, eds, *Global Administrative Law: The Casebook* (Institute for Research on Public Administration, 2012) 117.

availability and popularity of this video via an advertising model that capitalized on people searching for and viewing it.

The new *GDPR* in the EU would likely further require a hosting platform like Google Video to remove the video on request as part of the "right to be forgotten". The US consumer protection regime surely would not, because Google had no hand in creating or posting the video, nor did it specifically solicit this type of content, unlike the common practice on non-consensual pornography sites. The voluntary moderation guidelines leaked from Facebook in 2017 also reveal that photos mocking people with disabilities have until recently not been considered the kind of material that should be removed (the Facebook guidelines even included an image of a person with Down Syndrome as an example).[90] In other words, mocking people with disabilities is deemed a matter of freedom of speech, offensive but protected, although it is unclear in the guidelines and the discussion of them whether a request from the person pictured (or his or her guardian) would prompt a different action from Facebook than a general user's complaint about an objectionable image of an unknown person with disabilities.[91]

Identification is an aggravating factor in privacy invasion, and an online image of an identifiable person (*e.g.* showing a face) becomes something else entirely when that image is associated with a name. Images of an identifiable person may still contain sensitive personal information

90. Nick Hopkins, "Revealed: Facebook's internal rulebook on sex, terrorism and violence" *The Guardian* (21 May 2017), online: The Guardian <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence>; Julia Angwin & Hannes Grassegger, "Facebook's Secret Censorship Rules Protect White Men From Hate Speech But Not Black Children" *ProPublica* (28 June 2017), online: ProPublica <https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms>.

91. Nick Hopkins, "How Facebook allows users to post footage of children being bullied: Leaked guidelines on cruel and abusive posts also show how company judges who 'deserves our protection' and who doesn't" *The Guardian* (22 May 2017), online: The Guardian <https://www.theguardian.com/news/2017/may/22/how-facebook-allows-users-to-post-footage-of-children-being-bullied>.

(as with the autistic boy), but if the image is publicly associated with the name of a specific person, the degree of invasiveness is magnified. This distinction was described by Ghyslain Raza, a then 14-year-old boy who gained unwanted internet fame as the "Star Wars Kid" beginning in 2003, when a video he privately recorded of himself wielding a pretend lightsaber was found and posted by mocking classmates. He noted that it was only when his name was released by a media organization that the harassment became much worse, opening him up not only to bullying by people he already knew offline (his schoolmates) but also to random unknown individuals online.[92] So while many people have argued that the "Star Wars Kid" video entered public culture, along with its many benign user-generated variations, it is much more difficult to argue that the video and its variations should continue to be associated with Raza's name.[93]

This brings us back to the issue of name search results in search engines, and the way that Google, after the *Google Spain* decision, now distinguishes between requests to delist news articles that are, or are not, associated with a person. Even the newsworthiness of an article published by a dedicated news site wanes as time goes on if the individual named therein is no longer in the public eye.[94] Google lists 23 examples of news articles that were requested to be delisted and the decision it made in relation to each; in the 11 examples where Google granted the delisting, most dealt with articles referring to minor crimes, quashed convictions,

---

92. Rebecca Hawkes, "Whatever happened to Star Wars Kid? The sad but inspiring story behind one of the first victims of cyberbullying" *The Telegraph* (4 May 2016), online: The Telegraph <telegraph.co.uk/films/2016/05/04/whatever-happened-to-star-wars-kid-the-true-story-behind-one-of/>; Jonathan Trudel, "Return of the 'Star Wars Kid'", *Maclean's* (27 May 2013) 28.
93. Meg Leta Ambrose, "You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship" (2012) 17:07 International Review of Information Ethics 21; Limor Shifman, "An anatomy of a YouTube meme" (2012) 14:2 New Media & Society 187.
94. Meg Leta Ambrose, "It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten" (2013) 16:2 Stanford Technology Law Review 369.

crime victims or relatives of crime victims who were not public figures, as well as an article naming a contestant in a contest who was a minor at the time.[95] Of the 12 examples where delisting was not granted, most involved crimes by public officials, serious crimes, serious accusations regarding people in positions of trust, professional misconduct/discipline, fraud, and one example of a "media professional" requesting removal of links to articles reporting on embarrassing content he had posted himself.[96] Together, these examples show that Google has attempted to establish guidelines regarding what sort of personal information contained in news stories remains in the public interest enough to warrant ongoing public association with a person's name, and what does not.

While internet service providers, including Google, have not yet had to deal with the stronger right of erasure in the new *GDPR*, the key will be proportionality in balancing the public interest in access to information that has entered into public circulation against the ongoing privacy interests of the individuals named or otherwise identified. In some cases, an image — like the "Star Wars Kid" video — might acquire the status of a shared cultural document, the factual content of which is not particularly sensitive. In most others, determining whether delisting or deindexing is the most appropriate way to address the privacy interest of the subject will depend on both the degree of sensitivity of the information revealed (a child's autism-related reaction to physical confrontation is clearly more sensitive than a child's goofy playacting) and the degree to which the document in which the information appears has acquired or maintained newsworthiness (as distinguished from prurient or morbid curiosity)[97] or the public culture equivalent thereof. Widespread creative adaptation of a popular culture meme weighs in favour of keeping the Star Wars Kid video available, although it should be disassociated from the young man's

95. California passed a bill providing a means for minors to remove material they have posted themselves. See US, SB 568, *An Act to Add Chapter 22.1 (Commencing with Section 22580) to Division 8 of the Business and Professions Code, Relating to the Internet*, 2013–14, Reg Sess, Cal, 2015 (enacted).
96. Google Transparency Report, *supra* note 12.
97. Worley, *supra* note 13.

name unless he chooses otherwise, while mean-spirited humour found in the humiliation of a person with disabilities does not.

VI. Publicly Available ≠ Free for the Taking

Policies regarding how and whether to constrain businesses that profit from access to publicly available documents on the public internet have implications for how to regulate "big data", another front on which the privacy interests of data subjects may clash with business interests in monetizing publicly accessible information. These same authorities are beginning to question the idea that, although people leave behind a trail of information wherever they go and whatever they do online, this information is free for the taking. However, as with publicly accessible information packaged for open public consumption by information location services, to date regulators have only targeted the most egregious business practices.

For example, the FTC's 2015 decision and order against the website, Jerk.com, found the site operators to be engaging in unfair and deceptive business practices related to harvesting profile content from Facebook via an application program interface ("API") that allowed third-party application developers to access even content that was set to be shared only with "friends".[98] The operators of Jerk.com claimed that their content was created by their users, when in fact it was largely created by the operators themselves, from personal information scraped from Facebook and other "publicly accessible" sources, many of which contained full names and images, buttons for users to vote whether or not the person was a "jerk", and fields for users to fill in further information about that person.[99] These profiles were then made available for indexing by general search engines.[100] Jerk.com's business model included selling USD $30 memberships, requiring a USD $25 "customer service fee" to

98. US, Federal Trade Commission, *In the Matter of Jerk, LLC and John Fanning: Complaint* (No. 9361) (2014) at paras 7, 10–11 [Jerk.com Complaint].
99. US, Federal Trade Commission, *In the Matter of Jerk, LLC and John Fanning: Opinion* (No. 9361) (2015).
100. Jerk.com Complaint, *supra* note 98 at para 9.

communicate with administrators, and third-party advertising.[101]

The Respondents claimed that their enterprise amounted to speech protected by the First Amendment because the Facebook photos and profile information were "publicly available" and that Facebook was to blame for making that material accessible. In other words, once Facebook failed to ensure that its users' private information was protected, any developer could use that information however they chose.[102] Indeed the Respondent tried to argue that the First Amendment was implicated because the FTC's order impinges on "[j]erk.com posting publicly available information derived from the internet".[103] The FTC (and the US Court of Appeal that upheld its decision) rejected that claim, in essence finding that Jerk.com misrepresented the source of its profile content, thereby misleading consumers as to how it had obtained it.[104] The ruling is narrow, in that it does not directly deal with the problem of whether a business that exploits a technological weakness that renders personal information publicly accessible gains the right to process or package it in whatever way it pleases, provided that they are honest with consumers about the source.[105] It is unclear, then, whether the First Amendment would protect the right to publish personal information scraped from the internet via a security weakness, given the seminal 1989 US Supreme Court freedom of speech decision in *Florida Star v BJF*,[106] where a newspaper was permitted to defy restrictions on publicizing a rape victim's identity because police had been negligent in including her name in a police report. In that case, the onus on protecting sensitive personal information was placed entirely on the public authority that improperly released it; the distinction with the Jerk.com case could

101. *Ibid* at para 5.
102. Trial Brief of Respondent John Fanning in *Fanning v Federal Trade Commission* (No 15-1520) (2016) at 3, stating "nothing prohibited the publication on jerk.com information made accessible to the public by Facebook through the internet".
103. *Ibid*.
104. Jerk.com Complaint, *supra* note 98 at para 10.
105. US, Federal Trade Commission, *Fanning v Federal Trade Commission* (No 15-1520) (2016).
106. *Florida Star*, *supra* note 49.

come down to the difference between newsworthy material held by a public entity that media organizations utilized precisely as news upon its improper public release, versus private, non-newsworthy material that is improperly accessible and that has been utilized for a commercial purpose devoid of public interest.

In Canada, the OPC has made stronger statements about inappropriate exploitation of public access to personal information when it conducted an investigation into Google's data collection practices for its location-based services (Google Maps), where Google was discovered to have collected a significant amount of "payload data" from unencrypted WiFi networks in the course of the data-gathering operations of its Street View cars.[107] These data included the full names, telephone numbers, and addresses of many Canadians, as well as complete email messages, email headers, IP addresses, machine hostnames, and the contents of cookies, instant messages, and chat sessions.[108] While Google claimed that the data collection was inadvertent, the OPC nonetheless took the opportunity to stress that even if a WiFi network is unencrypted and therefore publicly accessible, that does not mean any private data travelling across that network are free for the taking:

> [n]otwithstanding the fact the personal information collected was sourced from unprotected networks (and was in some cases fragmented), it is impossible to conceive that a reasonable person would have considered such collection appropriate in the circumstances.[109]

What a reasonable person considers appropriate in the circumstances is the formula for determining commercial fairness in handling personal information set out in *PIPEDA*.[110] Further, Canadian constitutional protection for freedom of expression allows more restrictions regarding publication of sensitive personal information held by public authorities, even if it is "newsworthy" in the way that is understood in the US. The

---

107. Office of the Privacy Commissioner of Canada, *Google Inc WiFi Data Collection*, *PIPEDA* Report of Findings #2011-001 (Ottawa: OPC, 6 June 2011).
108. *Ibid* at para 17.
109. *Ibid* at paras 18, 21.
110. *PIPEDA*, *supra* note 14, ss 3, 5.

names of sexual assault victims, for instance, are routinely made subject to publication bans, even though their names are available to the public via court proceedings.[111] In other words, Canada does not place the onus only on data custodians to keep personal information from the public. Instead, Canada has mechanisms in place to impose obligations on publishers who have had access to that information where the sensitivity of the information warrants it, viewing such restrictions as justified in a free and democratic society: in other words, a fair restriction in grander terms.[112]

Many privacy scholars have expressed grave concerns about the ways that businesses are exploiting publicly accessible personal information, especially considering how little information these businesses make available about exactly how their information collection and packaging algorithms function.[113] Julie Cohen coined the term "biopolitical public domain", referring to the popular idea that all data are fair game and can be collected freely, which she sees as employing a skewed sense of the concept of "public domain" that operates in a more well-developed fashion in intellectual property law.[114] She argued that we need to develop a more robust notion of what belongs in the "data commons" with regard to the practices of information aggregators and processors, so as to better protect personal information even in the realm of publicly accessible raw or de-identified data.[115]

---

111. *Criminal Code*, RSC, 1985, c C-46, s 486.4.
112. *Canadian Newspapers Co v Canada (AG)*, [1988] 2 SCR 122.
113. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge: Harvard University Press, 2015); Tauel Harper, "The big data public and its problems: Big Data and the structural transformation of the public sphere" (2017) 19:9 New Media & Society 1424.
114. Julie Cohen, "The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy" (2017) Philosophy & Technology 1, online: Springer <link.springer.com/content/pdf/10.1007%2Fs13347-017-0258-2.pdf>.
115. *Ibid* at 12.

VII. Conclusion: Data Privacy in "Public"

Privacy scholars have begun to explore the various ways that publicly accessible information is being collected and used, both by public and private entities.[116] Unfair handling of publicly accessible personal information has a particularly potent adverse affect on historically or situationally vulnerable populations, further amplifying the urgency of a fairness-based approach to businesses that deal in such information. Public records that are easily accessible have the potential to be misused, disproportionally affecting the reputations and corresponding opportunities of members of historically marginalized groups, such as economically disadvantaged persons and historically persecuted ethnic minorities, as well as individuals who are vulnerable as a result of adverse life events. User-generated content is also more likely to disproportionately affect historically marginalized groups online, mainly due to the "subculture of humiliation" where users post derogatory, harassing information, often about disempowered groups (women, the poor, ethnic minorities, and persons with disabilities).[117] As Frank Pasquale wrote:

> [n]ew threats to reputation have seriously undermined the efficacy of health

116. Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement" (2003) 29:4 North Carolina Journal of International Law & Commercial Regulation 595; Danah Boyd & Kate Crawford, "Critical Questions For Big Data" (2012) 15:5 Information, Communication & Society 662; Kate Crawford & Jason Schultz, "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms" (2014) 55:1 Boston College Law Review 93 at 101; Levin, *supra* note 29; Amy Conroy & Teresa Scassa, "Promoting Transparency While Protecting Privacy in Open Government in Canada" (2015) 53:1 Alberta Law Review 175; Ramona Pringle, "'Data is the new oil': Your personal information is now the world's most valuable commodity" *CBC News* (25 August 2017), online: CBC <cbc.ca/news/technology/data-is-the-new-oil-1.4259677>.

117. OPC, "Online Reputation", *supra* note 78, citing Nicolaus Mills, "Television and the Politics of Humiliation" (2004) 51:3 Dissent 79 at 79; Emily B Laidlaw, "Online Shaming and the Right to Privacy" (2017) 6:1 Laws 1.

> privacy law, credit reporting, and expungement. The common thread is automated, algorithmic arrangements of information, which could render a data point removed or obscured in one records system, and highly visible or dominant in other, more important ones … [it] is not much good for an ex-convict to expunge his juvenile record, if the fact of his conviction is the top Google result for searches on his name for the rest of his life. Nor is the removal of a bankruptcy judgment from a credit report of much use to an individual if it influences lead generators' or social networks' assessments of creditworthiness, and would-be lenders are in some way privy to those or similar reputational reports.[118]

However, some scholars do not draw a parallel between business use of publicly accessible information and the kind of activities that search engines or other information location and packaging services do. For example, Neil Richards and Woodrow Hartzog noted that "[m]ost people are vastly less powerful than the government and corporate institutions that create and control digital technologies and the personal data on which those technologies run".[119] However both see the EU's "right to be forgotten" as a serious threat to online freedom of expression and access to information, which could create "[a]n internet that could be edited like Wikipedia by individuals who do not like the facts reported about them in newspapers".[120]

Freedom of expression remains an important component to determining when the privacy interests of data subjects should or should not prevail over public interest in access to an individual's personal information, whether commercial or not. But it is worth remembering that Google is a huge and diverse company, and that while *Google Spain*

---

118. Frank Pasquale, "Reforming the Law of Reputation" (2015) 47:2 Loyola University of Chicago Law Journal 515 at 516.
119. Neil Richards & Woodrow Hartzog, "Privacy's Trust Gap: A Review", Book Review of *Obfuscation: A User's Guide for Privacy and Protest* by Finn Brunton & Helen Nissenbaum, (2017) 126:4 Yale Law Journal 1181 at 1183.
120. *Ibid* at 1185; see also Neil M Richards, *Intellectual Privacy: Rethinking Civil Liberties In The Digital Age* (New York: Oxford University Press, 2015) at 90–92; Woodrow Hartzog, "A Stronger 'Online Eraser' Law Would Be a Mistake" *New Scientist* (6 November 2013), online: New Scientist <newscientist.com/article/mg22029420-200-a-stronger-online-eraser-law-would-be-a-mistake>.

is a decision that only affects its public search engine business, its parent company, Alphabet, is rapidly diversifying in a way that will make it increasingly difficult to separate out revenue derived from advertising linked to search results and revenue derived from data analytics more generally (*e.g.* connections between AdWords, AdSense, and YouTube, Google Maps, Gmail, Google Drive, and Google Play). What we decide to do in terms of characterizing information location and packaging services as either first and foremost business ventures, or as guardians of publicly available information, will affect regulations about the big data analytics industry and privacy going forward. Algorithms and other forms of machine learning and processing have inherent errors and biases. Therefore, imposing data protection obligations on businesses that use them to collect and package publicly accessible personal information can serve as a useful, if limited, means of addressing one variant of the machinations of informational power online.

Overall, however, all personal data collection, processing and packaging should be subject to an analysis rooted in fairness, regardless of whether that information is publicly accessible. That is, fairness requires an appropriate balance between competing interests, where the sensitivity of the information must be taken into account, including disproportionate impact on vulnerable populations, in order to determine what is a fair business practice in the ever-changing information marketplace.

When is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws

Normann Witzleb [*] **& Julian Wagner** [**]

The definition of "personal information" or "personal data" is foundational to the application of data protection laws. One aspect of these definitions is that the information must be linked to an identifiable individual, which is incorporated in the requirement that the information must be "about" or "relating to" an individual. This article examines this requirement in light of recent judicial and legislative developments in Australia, Canada and the European Union. In particular, it contrasts the decisions rendered by the Federal Court of Australia in Privacy Commissioner v Telstra Corporation Ltd *and by the European Court of Justice decisions in* Scarlet Extended *and* Patrick Breyer v Bundesrepublik Deutschland *as well as the new* General Data Protection Regulation *with Canadian law. This article also compares how the three jurisdictions deal with the vexed issue of IP addresses as personal information where the connection between the IP address and a particular individual often raises particular problems.*

---

* Normann Witzleb (Dr, LLB) is an Associate Professor at the Faculty of Law, Monash University, Melbourne, Australia. His research focus is on Australian and European private law, and in particular, the area of privacy rights, torts and remedies.

** Julian Wagner (Dr, LLM Eur.) is a Lecturer at the Faculty of Law (Chair of Prof Dr Spiecker gen. Döhmann, LLM), Goethe University, Frankfurt am Main, Germany. His research focuses on European law, environmental law and privacy law. His work was supported by a postdoc fellowship of the German Academic Exchange Service (DAAD).

I. Introduction
II. The Necessary Link between the Information and the Individual
A. Australian Law
1. The *Telstra* Determination by the Privacy Commissioner
2. The AAT Decision in *Telstra*
3. The Full Federal Court Decision in *Telstra*
4. Practical Consequences of the *Telstra* Litigation
B. Personal Information Under Canadian Law
C. European Union Law
1. Personal Data Under the European Data Protection Directive
2. Personal Data in the Case Law of the European Court of Justice
3. Changes Under the New General Data Protection Legislation
III. How Do Australia, Canada, and the European Union Deal with IP addresses as Personal Information?
A. Australian Approach
B. Canadian Approach
C. European Approach
IV. Conclusion

I. Introduction

Data protection laws aim to protect personal privacy by regulating the collection, processing and transfer of "personal information" (Australia and Canada), "personal data" (European Union) or "personally identifiable information" (United States). While the definitions of these terms vary across jurisdictions, what they have in common is that they are of fundamental significance. Data that does not contain information about an identified or identifiable individual in the sense of the respective definition falls outside the scope of data protection laws.

Differences in the definition of "personal information" have relevance not only for the application of domestic data protection laws but also affect data transfers between countries. Many domestic data protection regimes impose restrictions on the export of personal data to

a third country, particulary if the data protection level in that country is weaker than the law of the exporting state. This is intended to prevent the bypassing of national data protection laws by the transfer of data to a third country without an adequate level of protection. However, even if the substantive data protection laws of a third country provide a comparable level of protection overall, a closer look at the scope of application of its data protection regime may also be necessary. If a third country adopts a narrower understanding of the term "personal data", that country's privacy laws will not apply to some data that would be protected by the laws of the exporting country.

This article will analyse recent developments relating to these definitions in Australia and the European Union and provide a comparison with Canadian data privacy law. The article is prompted by an Australian appellate decision on the definition of "personal information" under the *Privacy Act*.[1] In its decision, *Privacy Commissioner v Telstra Corporation Ltd*,[2] the Full Court of the Federal Court of Australia also considered relevant Canadian jurisprudence. In particular, it referred to the decision of the Federal Court of Appeal in *Canada (Information Commissioner) v Canada (Transportation Accident Investigation & Safety Board)*.[3] This article will also consider recent developments in the European Union and, in particular, the new *General Data Protection Regulation* ("*GDPR*")[4] and two recent decisions of the European Court of Justice. The practical consequences of the differences between the terms will be explained using the example of the classification of Internet Protocol ("IP") addresses as personal information or as personal data, respectively.

---

1. *Privacy Act 1988* (Cth) (Austl) [Austl *Privacy Act*].
2. [2017] FCAFC 4 [*Telstra* FCAFC].
3. 2006 FCA 157 [*Canada (Information Commissioner)*].
4. EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [*GDPR*].

II. The Necessary Link between the Information and the Individual

The necessary link between the information in question and the individual differs in Australian, Canadian and European Union law.

A. Australian Law

Australia's federal data protection laws are contained primarily in the *Privacy Act*. The *Act* is informed by the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[5] and is mirrored in data protection laws in a number of Australian states and territories. The *Privacy Act* contains thirteen Australian Privacy Principles ("APPs"), which govern the collection, use, disclosure and storage of personal and sensitive information and how individuals may access and correct records containing such information. The APPs apply to most commonwealth government agencies and large private sector organisations (the so-called "APP entities").

The current definition of "personal information" in section 6 was inserted into the *Privacy Act* in 2014.[6] It states:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[7]

This represented a modernisation of the previous definition, which had been unchanged in the legislation since 1988 and defined (also in section 6) "personal information" as follows:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be

5. OECD Council, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (1980) [OECD Guidelines].
6. The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (Austl), took effect from 12 March 2014.
7. Austl *Privacy Act*, *supra* note 1, s 6(1).

ascertained, from the information or opinion.[8]

The new definition followed the recommendation of the Australian Law Reform Commission, which undertook a comprehensive review of Australian privacy laws in 2008.[9] The Explanatory Memorandum to the Amendment Bill explained that the amendment did not significantly change the scope of what is considered to be personal information.[10] In line with international standards, the new definition focuses on "identification" rather than the "identity" of the relevant individual. A related change is that it is no longer a requirement of the current definition that the person's identity must be apparent or reasonably ascertainable "from the information or opinion" itself. Information can now also be personal if it does not itself identify an individual but if it does so when combined with "other" information,[11] provided that the identification is reasonable. On that basis, it is likely that the new definition is "broader in scope than its predecessor".[12]

Most debate surrounding the definition of personal information is related to the issue of when a person is "identified" or "reasonably identifiable".[13] These discussions have become more important in light of

8. *Ibid*, as it appeared in 1988.
9. Austl, Commonwealth, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108) (ALRC, 2008) [ALRC, *For Your Information*].
10. Austl, Commonwealth, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Explanatory Memorandum* (2012) at 53 [Austl, Commonwealth, *Privacy Amendment Bill 2012 Explanatory Memorandum*].
11. Austl, Commonwealth, Office of the Australian Information Commissioner, *What is personal information?* (OAIC, 2017) at 7 [OAIC, *What is personal information?*].
12. Anna von Dietze & Anne-Marie Allgrove, "Australian privacy reforms: an overhauled data protection regime for Australia" (2014) 4:4 International Data Privacy Law 326 at 328.
13. See *e.g.* Anne SY Cheung, "Re-personalizing Personal Data in the Cloud" in Anne SY Cheung & Rolf H Weber, eds, *Privacy and Legal Issues in Cloud Computing* (Cheltenham: Edward Elgar Publishing, 2015) 69 at 69.

significant recent advances in re-identification technologies.[14] While de-identified information falls outside data protection laws, it has become contentious when information is sufficiently de-identified in the sense that, even with the use of re-identification technologies, individuals are no longer "reasonably identifiable".[15] However, this article will focus its attention on another aspect of the definition, *i.e.* the required linkage between the information and the person to which it is said to relate. This has previously been given less attention but was at the centre of the decision of the Australian Federal Court in the *Telstra* matter.

While the OECD Guidelines define personal data as "information relating to an identified or identifiable individual",[16] the Australian definitions — in their previous and current versions — refer to information "about" an individual. The Australian Law Reform Commission did not recommend a change to this formulation, noting that:

> although a number of international instruments use the term 'relates to', the *Privacy Act* terminology is consistent with the APEC Privacy Framework and reflects that fact that the information must be about an identified or reasonably identifiable individual.[17]

It has long been a matter of contention whether this formulation "about an individual" required a more direct link between the data and the individual than the formulation "relating to an … individual".[18] Any differences in meaning may be relevant in cases where information has

14. Jane Henriksen-Bulmer & Sheridan Jeary, "Re-identification Attacks—A Systematic Literature Review" (2016) 36:6 International Journal of Information Management 1184.
15. Council of Europe, Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, (2014) 0829/14/EN, WP216; Information and Privacy Commissioner, Ontario, Canada, "Big Data and Innovation, Setting the Record Straight: De-identification *Does* Work" , by Ann Cavoukian & Daniel Castro (Toronto: IPC, ITIF, 16 June 2014).
16. OECD Council, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) at Part I, 1. b).
17. ALRC, *For Your Information*, *supra* note 9 at para 6.51.
18. See *e.g.* Mark Burdon & Alissa McKillop, "The Google Street View Wi-Fi Scandal and its Repercussions for Privacy Regulation" (2013) 39:3 Monash University Law Review 702 at 712.

only a tenuous connection with an individual, and in particular where information identifies a device rather than an individual. In the *Telstra* litigation, this issue became central when a technology journalist named Ben Grubb sought access to the personal metadata held by Telstra, his mobile phone service provider. Telstra refused access to mobile network data that could be linked to Mr. Grubb only through cross-matching between the various databases, systems and networks which Telstra operated. The Australian Administrative Tribunal overturned the Privacy Commissioner's determination that the refusal to provide access to such metadata was in breach of privacy principles.[19] This decision was confirmed by the Full Court of the Federal Court.[20]

1. The *Telstra* Determination by the Privacy Commissioner

The *Telstra* decision grappled with the issue of whether the Australian definition contains two cumulative elements: first, that the data must be about a person; secondly, that the data must enable the identification of this person.[21] Before the decision of the Full Federal Court, the definition of personal information was considered in the 2008 inquiry by the Australian Law Reform Commission into Privacy Law and Practice[22] in

19. *Telstra Corporation Ltd v Privacy Commissioner*, [2015] AATA 991 [*Telstra* AAT].
20. *Telstra* FCAFC, *supra* note 2.
21. *Re Grubb and Telstra Corp Ltd*, [2015] AICmr 35 (Austl) [*Re Grubb*].
22. ALRC, *For Your Information*, *supra* note 9, ch 6.

a number of decisions of the Australian Administrative Tribunal[23] and in guidance notes of the Privacy Commissioner.[24] However, the notion of personal information had not been the subject of judicial analysis at the appellate level in Australia.

The opportunity for obtaining authoritative guidance arose from a privacy complaint by Mr. Grubb against Telstra. In 2013, when Australia's metadata retention legislation was being debated, Mr. Grubb sought access to all metadata that Telstra held about his mobile phone service. At that time, the (former) National Privacy Principle ("NPP") 6.1 in the *Privacy Act* gave individuals the right to access, subject to some exceptions, their own personal information held by an organisation, such as Telstra.[25]

When Telstra refused to provide access to all data requested, Mr. Grubb filed a complaint under section 36 of the *Privacy Act*. During an investigation by the Privacy Commissioner, Telstra provided access to further call data contained in billing records but continued to refuse access to some mobile network data, such as IP address information,[26]

---

23. *Re Lobo and Department of Immigration and Citizenship*, [2011] AATA 705 (concerning the definition of personal information in the *Freedom of Information Act 1982* (Cth) (Austl)); *Re Denehy and Superannuation Complaints Tribunal*, [2012] AATA 608. See also *WL v Randwick City Council (GD)*, [2007] NSWADTAP 58 (Austl) (concerning the definition in the *Privacy and Personal Information Protection Act 1998* (NSW) (Austl)); *WL v La Trobe University (General)*, [2005] VCAT 2592 (Austl) (concerning the definition in the (former) *Information Privacy Act 2000* (Vic) (Austl)); Mark Burdon & Paul Telford, "The Conceptual Basis of Personal Information in Australian Privacy Law" (2010) 17:1 Murdoch University Electronic Journal of Law 1.
24. Office of the Australian Information Commissioner, "APP guidelines" (February 2014) at paras B.79-B.88, online: OAIC <https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/archived/chapter-b-app-guidelines-v1.pdf>.
25. Austl *Privacy Act*, *supra* note 1 in the pre-2014 version.
26. That is a number that is assigned to and identifies Mr. Grubb's mobile device when it communicates with the internet.

Uniform Resource Locator ("URL") information[27] and cell tower data.[28] Telstra argued that "the metadata in dispute, which [sat] on its network management systems, [was] not personal information as defined under [section 6 of] the *Privacy Act*".[29] Telstra submitted that Mr. Grubb's identity was neither "apparent nor [could] it reasonably be ascertained from that data"[30] because it could allegedly only be linked to him through difficult and expensive cross-matching between the various databases, systems and networks Telstra operated. In May 2015, the Privacy Commissioner made a determination against Telstra under section 52 of the *Privacy Act*. The Commissioner held that Telstra's ability to provide this kind of data to law enforcement in a large number of cases was "indicative of its ability to ascertain with accuracy an individual's identity from metadata linked to that individual"[31] and further that, in light of Telstra's extensive resources, it was also reasonably able to ascertain it. On that basis, the Privacy Commissioner determined that the metadata in question was "personal information" and the refusal to provide access to it was "in breach of NPP 6.1".[32]

2. The AAT Decision in *Telstra*

On application by Telstra, the Administrative Appeals Tribunal ("AAT") of Australia set aside the Commissioner's determination. In a decision of December 2015, Deputy President Forgie did not primarily engage with the issue of whether Mr. Grubb was reasonably identifiable from the metadata held in Telstra's mobile network systems. Instead, she considered that the words "about an individual" in the definition of personal information raised a threshold issue. She stated that:

> the first step is to ask whether the information or opinion is about an individual. If it is not, that is an end of the matter. If it is, the second step in the

27. That is information that identifies the websites Mr. Grubb visited.
28. That is geo-location data that identifies from where Mr. Grubb used his mobile phone service.
29. *Re Grubb*, *supra* note 21 at para 34.
30. *Ibid*.
31. *Ibid* at para 83.
32. *Ibid* at para 106.

> characterisation process is to ask whether the identity of that individual "… is apparent or can reasonably be ascertained, from the information or opinion".[33]

This finding was surprising because both parties appeared to have proceeded on the basis that the determinative issue was whether Mr. Grubb's identity was apparent or could be reasonably ascertained from the information he sought access to. This assumption was in line with academic commentary that suggested that:

> in most cases, it may not be appropriate to talk of two separate (although cumulative) conditions for making data 'personal'; the first condition can be embraced by the second, in the sense that data will normally relate to, or concern, a person if it enables that person's identification. In other words, the basic criterion appearing in these definitions is that of identifiability – that is, the potential of data to enable [the] identification of a person.[34]

As a result of the *Telstra* litigation, this conventional wisdom no longer applies to Australia.

Forgie DP identified the required characterisation task with the following question: "Is the information about an individual being, in this case, Mr. Grubb or is it about something else"?[35] Adopting this approach, the Deputy President considered that the mobile network data generated by Mr. Grubb's calls or messages was "information about the service it provides to Mr. Grubb but not about him"[36] — notwithstanding the fact that the individual who obtained the service was ascertainable from this information. Such a binary characterisation appeared to disregard the possibility that information — just as it can be about more than one individual — can also be both about an individual and about a service provided to that individual. The decision did not elucidate how the distinction between information about an individual and information about something else was to be drawn, for example, when information is

---

33. *Telstra* AAT, *supra* note 19 at para 97 [emphasis in original].
34. Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014) at 129–30 (generally on the definitions of personal in international instruments).
35. *Telstra* AAT, *supra* note 19 at para 111.
36. *Ibid* at para 112 (this was despite the fact that, as the Deputy President accepted, the mobile network data may identify Mr. Grubb when combined with other data).

sufficiently related to an individual so as to be regarded as being "about the individual".

3. The Full Federal Court Decision in *Telstra*

The Privacy Commissioner formed the view that the AAT decision left too much uncertainty regarding the definition of "personal information" and appealed to the Federal Court. Privacy advocates welcomed this move because it provided the prospect of detailed judicial guidance by the Federal Court on this basic concept in Australia's privacy legislation. It was also hoped that the hearing would provide a forum to consider the extensive case law that has developed internationally on the meaning of personal information, and particularly in relation to metadata.

However, in a decision published in January 2017, the Full Court gave short shrift to the Privacy Commissioner's appeal, as well as to the application by two privacy organisations to be heard as *amici curiae*. The main judgment, delivered by Justices Kenny and Edelman (the latter now a judge of the High Court of Australia), held that the appeal concerned only one very "narrow question of statutory interpretation".[37] This was, whether the words "about an individual", in the pre-2014 version of section 6, had any substantive operation. Contrary to the submission on behalf of the Privacy Commissioner, the Court unanimously held that they did.[38] In doing so, Kenny and Edelman JJ (with whom Justice Dowsett agreed in a short judgment) endorsed the view of Forgie DP that the *Privacy Act* establishes a two-stage test for determining that information is personal information.

The Court did not examine whether the AAT had erred in its application of this definition to the facts, because in its view, no appeal ground had raised this for consideration.[39]As a result, it was not reviewed which of Mr. Grubb's mobile phone metadata was personal

37. *Telstra* FCAFC, *supra* note 2 at para 73.
38. *Ibid* at para 80.
39. *Ibid*.

information because it was "about" Mr. Grubb.[40] The fact that the Federal Court concentrated on a narrow, technical point dashed the expectations of privacy professionals that the decision might become a landmark judgment that would fully resolve the issues raised in the AAT decision. Nevertheless, the Court provided some observations on how the definition of "personal information" operates in practice. The Privacy Commissioner decided not to appeal the matter to the High Court, which makes it pertinent to review these comments on the operation of the definition.

Kenny and Edelman JJ stated:

> [t]he words "about an individual" direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. Information and opinions can have multiple subject matters. Further, on the assumption that the information refers to the totality of the information requested, then even if a single piece of information is not "about an individual" it might be about the individual when combined with other information. However, in every case it is necessary to consider whether each item of personal information requested, individually or in combination with other items, is about an individual. This will require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity can reasonably be ascertained will require an evaluative conclusion.[41]

4. Practical Consequences of the *Telstra* Litigation

The clarification by the Full Court in *Telstra* that information can have multiple subject matters is welcome because, as discussed above, the approach adopted by the AAT appeared to suggest that the characterisation task is black-or-white — *i.e.* that information will be either about an individual or about something else. The judgment of Kenny and Edelman

40. The enactment of the mandatory data retention legislation through the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (Austl) has put this question beyond doubt because the *Telecommunications (Interception and Access) Act 1979* (Cth) (Austl) now contains an express provision (s 187LA) that metadata required to be retained by the telecommunications provider is taken to be "personal information" for the purposes of the *Privacy Act*.

41. *Telstra* FCAFC, *supra* note 2 at para 63.

JJ also clarifies that the assessment of whether the individual's identity is apparent or can be ascertained must take into account other information with which the information in question can be combined.[42]

However, because of the way the appeal was argued, the Federal Court was not obliged to provide further assistance on how the evaluative task is to be undertaken.[43] In particular, the Court left open, just as the AAT did, the approach to determining the issue of when the link between information and an individual is so tenuous that it cannot be said that the information is "about an individual". Kenny and Edelman JJ gave as an example that the colour of Mr. Grubb's mobile phone was not information they considered to be about him, but they did not explain *why* this was not the case.[44]

The difficulties posed by the characterisation task can be illustrated with the common example of IP addresses. IP addresses were part of the metadata requested by Mr. Grubb, and their characterisation as personal data is a vexed issue also in other jurisdictions. An IP address is allocated by the Internet Service Provider ("ISP") to a subscriber's device so that a particular communication on the internet can be delivered to that device. It is standard practice for many website operators to log the IP addresses of webpage visitors, which raises the question of whether these data logs are personal information and, therefore, fall under data protection legislation. Most connections rely on dynamic IP addresses, which are assigned by the ISP whenever the device connects to the internet and which change regularly. An IP address identifies a specific network device rather than the individual using that device, and dynamic IP addresses may change over time. On that basis, Forgie DP held that a dynamic IP address is not information about an individual because "[t]he connection between the person using a mobile device and an IP address is … ephemeral".[45] The Deputy President did not consider, however, that information, even when it is not directly about an individual, may become personal if it may be linked to an individual through indirect means, such

42. *Telstra* FCAFC, *supra* note 2.
43. *Ibid*.
44. *Ibid*.
45. *Telstra* AAT, *supra* note 19 at para 113.

as through the interrogation of and matching across multiple databases. The decision of the Federal Court suggests that a more nuanced approach may be needed, in particular one that considers whether the information, in combination with other information, is to be regarded as being "about an individual".[46]

It is important to note that the judgment of the Federal Court concerned the definition of "personal information" as it applied before March 12, 2014. Since that date, the definition has been amended to "… information or an opinion about an identified individual, or an individual who is reasonably identifiable …", so as to align it more closely with international legal instruments.[47] NPP 6.1 has been replaced by Australian Privacy Principle 12.1, which adopts different language but is otherwise similar. Despite these changes in the wording, the Court's reasoning is likely to remain applicable because the current definition retains that the information or opinion must be "about an … individual".[48] A key difference between the old and the current definition of personal information is that the individual no longer needs to be identifiable "from the information or opinion". In relation to the old definition, Kenny and Edelman JJ stated that:

> whether information is "about an individual" might depend upon the breadth that is given to the expression "from the information or opinion". In other words, the more loose the causal connection required by the word "from", the greater the amount of information which could potentially be "personal information" and the more likely it will be that the words "about an individual" will exclude some of that information from National Privacy Principle 6.1.[49]

It is unclear what significance these comments have for the purposes of

---

46. As will be discussed below, this is also the position taken under the equivalent provisions in the European Union. See *e.g.* the recent decision of the European Court of Justice in the case of *Patrick Breyer v Bundesrepublik Deutschland*, [2016] EUECJ C-582/14 [*Breyer*] (in relation to website operators) and previously *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, [2011] EUECJ C-70/10 [*Scarlet Extended*] (in relation to ISP providers).
47. ALRC, *For Your Information*, *supra* note 9 at para 6.53.
48. Austl *Privacy Act*, *supra* note 1, s 6(1).
49. *Telstra* FCAFC, *supra* note 2 at para 64 [emphasis in original].

the new definition, which no longer contains the limiting expression "from the information or opinion". It would be concerning if this was understood to attribute an even more significant exclusionary function to the words "about an individual".

Unfortunately, the *Telstra* litigation has provided few new insights on when information is to be considered "personal information" under the *Privacy Act*. In many cases, information will fall clearly either within or outside the definition of "personal information". As far as metadata held by telecommunications providers under the mandatory data retention laws is concerned, the matter was put beyond doubt through statutory deeming provisions. The issue remains live in other contexts, however, such as when businesses or other organisations employ cookie technology to record the IP addresses of website visitors.[50] The classification also continues to be difficult when information (such as internal business data) does not directly identify any individual but can be linked to individuals through indirect means, such as data matching across databases.[51] In cases of doubt, the Office of the Australian Information Commissioner advises organisations and agencies in updated guidance notes to err on the side of caution and treat this information as personal information.[52] This recommendation confirms that the definition of "personal information" — described by the Privacy Commissioner as "arguably the most important term in the *Privacy Act*"[53] — remains in significant respects uncertain.

The Explanatory Memorandum to the *Privacy Enhancement Bill* stated that the amendment "also brings the definition in line with

50. See Robert Slattery & Marilyn Krawitz, "Mark Zuckerberg, the Cookie Monster – Australian Privacy Law and Internet Cookies" (2014) 16:1 Flinders Law Journal 1.
51. See *e.g. Waters v Transport for NSW*, [2018] NSWCATAD 40 (Austl) (considering the collection of personal information by Transport for NSW users of the electronic travel card system "Opal").
52. OAIC, *What is personal information?*, *supra* note 11 at 17.
53. Timothy Pilgrim, "Privacy Awareness Week Launch 2016" Office of the Australian Information Commissioner (16 May 2016), online: OAIC <https://www.oaic.gov.au/media-and-speeches/speeches/privacy-awareness-week-launch-2016>.

international standards and precedents".[54] On that basis, it was expected that the revised definition of personal information would be "interpreted with regard to its counterparts in the EU and elsewhere".[55] This, however, did not occur in *Telstra* FCAFC.[56] In fact, the Full Court was highly critical of the submission of the prospective *amici curiae* that sought to draw the Court's attention to international data protection sources. The Court took particular issue with reliance on overseas materials which concerned "legislation which was worded differently, and based upon a different context and background even though ultimately deriving from the same broadly worded international instruments".[57] Unfortunately, the decision of the Full Court does not seem to acknowledge the degree of international consensus on the basic definitions of data privacy legislation and the fact that Australia's legislation was expressly intended to reflect settled international practice.

It is correct that the international instruments have varying character. The OECD Guidelines maintain a high degree of flexibility and do not seek to provide the adoption of a particular approach. In their Explanatory Memorandum, it is stated that the "precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country".[58]

The next section of the article will explore the Canadian definition of personal information. Of all of the international material presented to the Full Court, the Court was most drawn to Canadian jurisprudence. In particular, the decision in *Canada (Information Commissioner)*[59] was described as "the most relevant, indeed the only potentially relevant, authority".[60] The next section will, therefore, analyse the Canadian

54. Austl, Commonwealth, *Privacy Amendment Bill 2012 Explanatory Memorandum*, *supra* note 10 at 53.
55. Dietze & Allgrove, *supra* note 12 at 328.
56. *Telstra* FCAFC, *supra* note 2 at para 71.
57. *Ibid*.
58. OECD Guidelines, *supra* note 5 at 41.
59. *Canada (Information Commissioner)*, *supra* note 3.
60. *Telstra* FCAFC, *supra* note 2 at para 74.

definition of personal information.

B. Personal Information Under Canadian Law

In Canada, the right to privacy is protected under section 8 of the *Canadian Charter of Rights and Freedoms* ("*Charter*"), which creates a right to be secure against unreasonable search or seizure.[61] There are a number of mechanisms at the federal and provincial level that protect information privacy. The most important federal statutes are the *Privacy Act*[62] and the *Personal Information Protection and Electronic Documents Act*[63] ("*PIPEDA*"). The *Privacy Act* governs the personal information handled by federal government institutions, whereas the *PIPEDA* applies to private sector entities that collect, use or disclose personal information in the course of commercial activities.[64] Both *Acts* define personal information as "information about an identifiable individual",[65] or, in the equally binding French language version, as "tout renseignement concernant un individu identifiable".[66] One of the drivers of the introduction of the

61. The *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 8 [*Charter*].
62. *Privacy Act*, RSC 1985, c P-21 [Canada *Privacy Act*].
63. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
64. There are also a number of provincial statutes, including the *Personal Information Protection Act*, SBC 2003, c 63; *Personal Health Information Protection* Act, SO 2004, c 3, Schedule A; *Loi sur* la protection des *renseignements personnels dans* le *secteur* prive, CQLR c P-39.1.
65. Canada *Privacy Act*, *supra* note 62, s 3 contains further specification for the purposes of this Act, including that the information is "recorded in any form". The definition wording, "information about an identifiable individual that is recorded in any form" is also contained in the *Model Code for the Protection of Personal Information, National Standard of Canada* CAN/CSA-Q830-96 at 1.
66. *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, s 2(1) [*LPRDE*].

PIPEDA was the European Data Protection Directive,[67] which prohibits the transfer of personal data to third countries that do not have adequate levels of privacy protection for personal information.[68]

The definition of personal information has been central in a number of judicial decisions and determinations of data protection commissioners. In *Dagg v Canada (Minister of Finance)*, Justice La Forest described the definition in the *Privacy Act* as "undeniably expansive" and intending "to capture *any* information about a specific person, subject only to specific exceptions".[69] According to the Privacy Commissioner, the word "about" in the *PIPEDA* definition of personal information means that the information is "not just the subject of something but also *relates* to or *concerns* the subject".[70] Initially, the Privacy Commissioner interpreted this requirement rather narrowly. In a finding released in 2001, the Office of the Privacy Commissioner ("OPC") determined that the information contained in an individual prescription was not associated sufficiently with the physician who wrote it to qualify as

67. EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31 [EC, *Directive 95/46/EC*].

68. See *AT v Globe24h.com*, 2017 FC 114 at para 49; Council of Europe, Article 29 Data Protection Working Party, *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act*, (2001) 5109/00/EN, WP39.

69. *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at paras 68–69 [emphasis in original]; see also *Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 at para 23 [emphasis in original].

70. Office of the Privacy Commissioner of Canada, "PIPEDA Interpretation Bulletin: Personal Information" (October 2013), online: OPC <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/> [emphasis added].

personal information "about" the physician himself.[71] This conclusion drew heavily on the consideration that a prescription is the outcome of a professional interaction between the involved physician and the treated patient, rather than a description of the physician himself or his activities apart from the fact that he issued the prescription.[72] The OPC further referred to the purpose of the *PIPEDA*, as laid down in section 3, as an *Act* to recognise the right of privacy of individuals which, according to the OPC, does not, when balanced against legitimate commercial purposes, cover information that is only the result of the work activity of an individual.[73] But subsequently, the OPC altered its position to a wider, contextual approach on the scope of the term "about". Apart from the context of information production, the OPC now also takes into account the context of the information collection, its use and disclosure.[74]

In 2003, the OPC decided that sales statistics of individual employees are not only part of the company information a company generates but also reveal the on-the-job performance of individuals and, therefore, also qualify as personal information under the *PIPEDA*.[75] In a comparable case in 2005, the OPC decided that the sales records of independent real estate agents were commercial information connected with their conducted business as well as personal information concerning the individual real

71. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2001-15" (2 October 2001), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/wn_011002/>.
72. *Ibid*.
73. *Ibid*.
74. Office of the Privacy Commissioner of Canada, "The Privacy Commissioner of Canada's Position at the Conclusion of the Hearings on the Statutory Review of PIPEDA" (November 2006), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2007/sub_070222_03/> [PCC, "The Privacy Commissioner of Canada's Position"].
75. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2003-220" (15 September 2003), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-220/>.

estate agent.[76] The OPC also decided that information about property is personal information if it reveals something of a personal nature about an individual.[77] For example, the purchase price of real estate in post-sale advertising could reveal personal traits of the buyer, such as her abilities to pay or to bargain.[78]

Of the judicial determinations, the decision in *Canada (Information Commissioner)*, which the Australian Federal Court referred to, stands out. The matter concerned refusals by the Canadian Transportation Accident Investigation and Safety Board to disclose records in reliance on the "personal information" exception in section 19 of the *Access to Information Act*.[79] Subsection 19(1) of the *Act* prohibits the disclosure of "personal information as defined in section 3 of the *Privacy Act*".[80] The records in question were recordings and/or transcripts of air traffic control communications relating to four aviation occurrences, which were subject to investigations and public reports by the Safety Board.

Justice Desjardins (with whom Chief Justice Richard and Justice Evans agreed) conducted a two-tier test to determine whether data is "personal information".[81] Firstly, the data has to be about an individual. Secondly, the data has to permit or lead to the possible identification of the individual. The two elements "about" and "identifiable individual" have to be met cumulatively for any data to be seen as personal information

---

76. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2005-303" (31 May 2005), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-303/>.
77. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2006-349" (24 August 2006), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-349/>.
78. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2009-002" (20 February 2009), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-002/>.
79. *Access to Information Act*, RSC 1985, c A-1.
80. *Ibid*, s 19(1).
81. *Canada (Information Commissioner)*, *supra* note 3.

under Canadian law.[82] In Desjardins JA's view, the two words "about" and "concernant" "shed little light on the precise nature of the information which relates to the individual".[83] However, her Ladyship added that the term "personal information" has to be understood "as equivalent to information falling within the individual's right of privacy" because the purpose of data protection laws is to protect this right of privacy of individuals.[84] Hence, any information can only be understood as "about" an individual when it involves subjects that "engage [an individual's] right to privacy",[85] which is said to connote "concepts of intimacy, identity, dignity and integrity of the individual".[86]

In a statement reminiscent of the Australian Full Court decision, Desjardins JA observed:

> [t]he information at issue is not "about" an individual … the content of the communications is limited to the safety and navigation of aircraft, the general operation of the aircraft, and the exchange of messages on behalf of the public. They contain information about the status of the aircraft, weather conditions, matters associated with air traffic control and the utterances of the pilots and controllers. These are not subjects that engage the right of privacy of individuals.[87]

In *Canada (Information Commissioner)*, the Court ruled that the disputed recordings and transcripts of air traffic control communications indeed enabled the identification of individual people and assisted in a determination as to how they performed their specific tasks in a certain situation. However, the information did not thereby qualify as personal information because the content of the information only affected their

---

82. However, the subsequent decision of Gibson J in *Gordon v Canada (Health)*, 2008 FC 258 appears to elide the two cumulative requirements when it states that ("information [is] "about" a particular individual if it "permits" or "leads" to the possible identification of the individual, whether alone or when combined with information from sources "otherwise available" including sources publicly available" at para 33).
83. *Canada (Information Commissioner)*, *supra* note 3 at para 43.
84. *Ibid* at paras 44–48.
85. *Ibid* at para 53.
86. *Ibid* at para 52.
87. *Ibid* at para 53.

"professional and non-personal nature"[88] and therefore "[did] not match the concept of "privacy" and the values that concept [was] meant to protect".[89] Access to the recordings could therefore not be withheld on the basis of the "personal information" exception. There are also a number of access of information cases at the provincial level that made a distinction between information "about" an individual and information "about" something else,[90] in particular where the information related to an individual acting in their professional or official capacity.

However, another access to information decision of the Federal Court of Appeal a year later demonstrates that these determinations can include fine distinctions. In *Janssen-Ortho Inc v Canada (Minister of Health)*,[91] the Court held that the documents revealing the names and business contact information of employees of the appellant company, as well as the views they expressed to Health Canada on the withdrawal of a prescription drug from the Canadian market, constituted the personal information of these employees. In *Husky Oil Operations Limited v Canada-Newfoundland and Labrador Offshore Petroleum Board*,[92] the Federal Court of Appeal recently suggested that these two decisions are not inconsistent but can be explained by differences in the nature of the information concerned. Justice Montigny (Justice Wood concurring) also affirmed that a purposive approach "best carries out Parliament's intent in adopting the *Access Act* and the *Privacy Act*".[93] However, each of the Acts using the definition of personal information, the *Access to Information Act*, the *Privacy Act* and *PIPEDA* differ in their statutory objectives, particularly in relation to the balance between personal privacy and the

88. *Ibid* at para 54.
89. *Ibid*.
90. See further, Teresa Scassa, "Geographical Information as 'Personal Information'" (2010) 10:2 Oxford University Commonwealth Law Journal 185 at 194–96.
91. *Janssen-Ortho Inc v Canada (Minister of Health),* 2007 FCA 252 aff'd in *Information Commissioner of Canada v Canada (Natural Resources)*, 2014 FC 917.
92. *Husky Oil Operations Limited v Canada-Newfoundland and Labrador Offshore Petroleum Board*, 2018 FCA 10.
93. *Ibid* at para 45.

other objectives they need to be fulfilled. Under a purposive approach to the definition of personal information, it can be argued that the degree of connection required between the information and the individual may need to differ between privacy and access-to-information cases,[94] despite the fact that the *Access to Information Act* adopts the definition in the *Privacy Act*.

In conclusion, the Canadian definitions of personal information in the *Privacy Act* and the *PIPEDA* have the cumulative requirements that the information allows the identification of an individual and that it is also "about" an individual, which requires an evaluation of the link between the information and the individual. The evaluative task is to be undertaken by reference to the purpose of the legislation. Where information does not involve subject-matter that engages an individual's privacy rights, the information is not personal information, even if it may identify an individual. However, this determination can make difficulties in some cases, particularly where it is unclear whether the information affects an individual in a personal capacity.

C. European Union Law

It has been acknowledged that the European Data Protection Directive ("DPD"),[95] which was in force from 1995 until its replacement with the General Data Protection Regulation in May 2018, had a "major transformational impact" on Canadian privacy law.[96] One of the main indicators of the influence of the European Union data privacy regime on Canada is the similarity of the definitions used in the DPD and the *PIPEDA*. According to the Canadian Privacy Commissioner, the "key goal in drafting the definition of personal information in the *PIPEDA* was to ensure that Canadian law was harmonized with European law".[97] The harmonisation of Canadian and European Union law through the

94. Scassa, *supra* note 90 at 197–98 and 209–10.
95. EC, *Directive 95/46/EC*, *supra* note 67.
96. Jennifer McClennan & Vadim Schick, "'O, Privacy' Canada's Importance in the Development of the International Data Privacy Regime" (2006) 38:3 Georgetown Journal of International Law 669 at 671.
97. PCC, "The Privacy Commissioner of Canada's Position", *supra* note 74.

adoption of similar terminology and a similar level of protection was intended to avoid obstacles for transatlantic trade.[98]

The definition of personal information in section 2(1) of the *PIPEDA* as "information about an identifiable individual"[99] picks up not only on the Canadian *Privacy Act* but also on the DPD.

1. Personal Data Under the European Data Protection Directive

The English language version of Article 2 of the DPD provided that:

> "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly …[100]

This article closely resembled the Canadian definition as described above, even though the wording differs slightly. The *PIPEDA* uses the word "about" to describe the necessary link between the information and the individual, while the DPD uses the term "relating to". The similarity between the Canadian and European definition is even more apparent in the respective versions in the French language. In section 2(1) of the *PIPEDA*, personal information is described as "tout renseignement concernant un individu identifiable",[101] whereas the French version of the DPD defined personal data as "toute information concernant une personne physique identifiée ou identifiable".[102] In other words, both jurisdictions made use of the word "concernant" to describe the necessary link.

This definition of personal data within the DPD shows that European Union law also demanded that the information in question must relate to the individual to qualify as personal data. This is also in line with Article

98. *Ibid*.
99. *PIPEDA*, *supra* note 63, s 2(1).
100. EC, *Directive 95/46/EC*, *supra* note 67, art 2(a).
101. *LPRDE*, *supra* note 66, s 2(1).
102. EC, *Directive 95/46/CE du Parlement européen et du conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [1995] OJ, L 281/31, art 2(a).

2(a) of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* ("*Convention 108*"), which defines "personal data" as "any information relating to an identified or identifiable individual".[103] This *Convention* is a Council of Europe treaty to which all member states of the European Union are bound. The DPD (as well as the new *GDPR*) are considered to be acts implementing the *Convention 108*, as the European Union now exercises the legislative power in the field of privacy law which was previously assigned to its member states.[104]

It is unclear what kind of connection between the information in question and an individual is required under the DPD (and now the *GDPR*) to link the information to the individual being. Some scholars assume that under European Union law, the term "relating to" has no discrete meaning and thus is generally fulfilled if the data reveals an identified or identifiable data subject.[105] However, a closer look reveals a more complex situation. A Working Paper on the concept of personal data issued by the Article 29 Working Party (an advisory body established

103. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, Eur TS 108 (entered into force 1 October 1985), art 2(a) [*Convention 108*].

104. On the obligations of the EU in relation to treaties signed by its member states, see *International Fruit Company NV v Produktschap voor Groenten en Fruit*, [1971] EUECJ R-54/71 at para 14 *et seq*.

105. On the DPD, see Bygrave, *supra* note 34 at 129–30; Paul M Schwartz & Daniel P Solove, "Reconciling Personal Information in the United States and European Union" (2014) 102:4 California Law Review 877. On the *GDPR*, see Stefan Ernst in Boris P Paal & Daniel A Pauly, eds, *Datenschutz-Grundverordnung* (Munich: Beck, 2017), art 4 at paras 3 *et seq*; Hans-Hermann Schild in Heinrich A Wolff & Stefan Brink, eds, *Beck'scher Online-Kommentar Datenschutzrecht*, 20 ed (Munich: Beck, 2017) (loose-leaf consulted on 30 August 2017), art 4 at paras 3 *et seq*. Both of these commentaries do not consider the term "relating to" in any detail.

under the DPD[106]) provides further guidance as to how this term shall be interpreted.[107] The Working Party stated that "[i]n general terms, information can be considered to 'relate' to an individual when it is *about* that individual".[108]

The Working Party's Opinion first identifies situations in which it is self-evident that information relates to an individual, such as the information contained in one's personnel file or medical file, or images of a person's video interview. It then deals with situations in which it is more difficult to establish the relationship between information and an individual, such as when the data concerns objects, processes or events in the first place, not individuals.[109] Also, in these cases the information can "indirectly" or "in some circumstances" relate to an individual. The Opinion identifies three key elements — the content element, purpose element and result element — and suggests that at least one element is required to establish the necessary connection.[110]

The "content" element is fulfilled when information is given about a particular individual. To determine if the link between the content of the information is close enough to establish such a connection, one has

106. The Article 29 Working Party was an independent advisory body composed of representatives of the data protection supervisory authorities of each Member State, the European Data Protection Supervisor and the European Commission. Its functions included to advise the European Commission and to contribute the uniform application of data protection rules throughout the European Union: *cf.* recital 65 of the DPD. Upon entry into force of the *GDPR*, it has been replaced by the European Data Protection Board, see art 68.

107. Council of Europe, Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, (2007) Working Paper 136 [Opinion 4/2007].

108. *Ibid* at 9 [emphasis in original].

109. *Ibid*.

110. *Ibid* at 10 *et seq*. Similarly, see Information Commissioner's Office, "Determining what is personal data" (2007), online ICO <https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>; Martin Eßer in Martin Eßer, Philipp Kramer & Kai von Lewinski, eds, *Auernhammer DSGVO BDSG*, 6 ed (Cologne: Carl Heymanns, 2018), art 4 at paras 10–11.

to take into account all circumstances of the case and the meaning of the word "relate" in the general non-juridical linguistic usage.[111]

The "purpose" element is present when the disputed information is used or is likely to be used with the purpose of evaluating or treating an individual on this basis of this information in comparison to other individuals.[112]

Finally, the "result" element can be considered to exist when the use of the information in question is likely to have an impact on the rights and interests of a certain individual. The result does not necessarily have to be of major impact but rather it is sufficient if the individual may be treated differently compared to other individuals as a result of processing that data.[113]

The Working Party gives the example of data concerning a taxi's location which is collected by the taxi company for the purpose of fleet management, providing a better service to the customers and saving fuel by allocating the closest taxi to the customer. The content of the geolocation data, according to the Working Party, is only connected with the taxi cars, not the drivers, and its purpose is only to enhance business processes. However, because of the necessary link between the geolocation information about a taxi and the person who is driving it, the data allows the monitoring of the performance of the taxi drivers themselves. Therefore, under the application of the purpose element, the data is to be considered personal data of the taxi driver.[114]

The overall conclusion from the Opinion is that the Article 29 Working Party interprets the meaning of the term "concerning", as used in the DPD, in a rather wide sense, especially in comparison to the Australian and Canadian understanding of personal information. It does not only include data that is directly about a particular person but also data that is used for the purpose of differential treatment of that person to another or is otherwise likely to have some impact on the rights of a person.

111. Opinion 4/2007, *supra* note 107.
112. *Ibid*.
113. *Ibid* at 11.
114. *Ibid*.

It is, therefore, sufficient if the data allows any conclusions about an individual to be drawn or if the data is collected with such an objective in mind. A further consequence of this broad notion of personal data is that a specific piece of information can represent the personal data of more than just one person at the same time.[115]

2. Personal Data in the Case Law of the European Court of Justice

The case law of the European Court of Justice ("ECJ") supports, at least indirectly, this broad interpretation given by the Article 29 Working Party. In the two decisions of *Scarlet Extended* and *Breyer*, the ECJ dealt with IP addresses and ruled that they are generally protected personal data.[116] In these decisions, the Court did not touch on the issue of whether IP addresses are information relating only to an electronical device, rather than the human being using the device. Instead, the ECJ focused only on the question of whether an individual can be reasonably identified on the basis of an IP address.[117] The focus in both decisions on the criterion of identifiability in the DPD's legal definition of personal data suggests that the necessary link between the data in question and the individual, as required by the criterion in Article 2 of the DPD that the data must "relate to" the individual, is fairly low.

In its interpretation of the term personal information, the ECJ did not expressly consider comparative materials, despite the fact that the definition has international counterparts including international agreements, such as the *Convention 108* as mentioned above, and the law of Canada. This is, however, in line with the other judgments rendered by the ECJ in which the Court showed a reluctance to engage with third

115. *Ibid* at 12.

116. *Scarlet Extended*, *supra* note 46 at para 51; *Breyer*, *supra* note 46 at paras 38 *et seq*.

117. *Breyer*, *supra* note 46 at para 39.

country law in its reasoning.[118]

3. Changes Under the New General Data Protection Legislation

The DPD has been replaced with the new *General Data Protection Regulation* ("*GDPR*") since May 2018.[119] The main driver for this change was the desire to have a uniform level of data protection between the European Union member states which existed under the old DPD. According to Article 288 paragraph 2 of the *Treaty of the Functioning of the European Union* ("*TFEU*"), a European Union regulation is binding in its entirety and directly applicable in all European Union member states.[120]

The English language version of the definition of personal data in Article 4 paragraph 1 of the new *GDPR* remains largely unchanged compared to the DPD and, in particular, still requires the information to be "relating to" an identifiable natural person.[121] Interestingly, the French definition now utilizes the term "se rapportant" instead of the former "concernant" to describe the necessary connection. Although

---

118. *Cf.* Christopher Kuner, "Third Country Law In The CJEU's Data Protection Judgments" *European Law Blog* (12 July 2017), online: European Law Blog <https://europeanlawblog.eu/2017/07/12/third-country-law-in-the-cjeus-data-protection-judgments/>.
119. *GDPR*, *supra* note 4.
120. *Cf. Ibid* at paras 9–13; Paul de Hert & Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" (2016) 32:2 Computer Law & Security Review 182; Peter Schantz, "Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht" (2016) 69:26 Neue Juristische Wochenschrift 1841.
121. However, it is worth mentioning that the scope of the definition was expanded by lowering the requirements for the identification of an individual. *Cf.* Bert-Jaap Koops, "The Trouble with European Data Protection Law" (2014) 4:4 International Data Privacy Law 250; Bert van der Sloot, "Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation" (2014) 4:4 International Data Privacy Law 307; Schwartz & Solove, *supra* note 105.

all language versions are equally authentic in European Union law,[122] and therefore the alteration of the wording of an article in one of the language versions might indicate a different meaning, the proposal for the *GDPR* was originally drafted (only) in English. This suggests that no amendment to the legal definition of personal data was intended by the introduction of the *GDPR*. This view is supported by the fact that the Explanatory Memorandum to the draft of the *GDPR* did not address this modification of the definitional text.[123] Like its predecessor, the *GDPR* does not provide clarification of the term "relating to". Recital 26 of the *GDPR* only repeats recital 26 of the DPD and goes to great lengths to explain how to determine whether a person is identifiable but does not explain when the link between the data and an individual is close enough so that data is "relating to" the person.[124]

In conclusion, the most authoritative guidance on this issue remains the working paper of the Article 29 Working Group referred to above. According to this, data "relates to" an individual under European Union data protection law when the data is likely to have an impact on the individual or her position in comparison to others or the data can be used to describe the individual in one way or another. In doing so, the European Data Protection framework only makes low demands on the necessary link between the data in question and an individual to categorise the data as personal data under European Union law. As the Canadian definition of personal information is derived from the European notion, an argument could be made that this understanding would also be a suitable starting point for the interpretation of the Canadian term. However, this position is currently not reflected by Canadian case law interpreting the *PIPEDA* definition, which does not refer to European Union law or its understanding by the ECJ.

---

122. *Cf. Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health*, [1982] EUECJ R-283/81 at paras 18 *et seq*.
123. EC, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final* at 7.
124. *GDPR*, *supra* note 4.

III. How Do Australia, Canada, and the European Union Deal with IP addresses as Personal Information?

This different understanding of the terms "about" or "relating to" in Australian, Canadian and EU law leads to a different comprehension of personal data, respectively personal information which, in turn, affects the scope of application of the respective data privacy regimes. The stricter the requirements for the connection between the information and the affected individual, the narrower the term of personal data or personal information ought to be understood. This, in turn, results in a narrower scope of application of the respective data protection legislation. Accordingly, the European data protection law which requires only a tenuous connection between the two elements has a broader scope of application than the Canadian and Australian data protection law.

This can be clearly illustrated using the example of IP addresses, which form the backbone of electronic communication. IP addresses are used to allow the clear identification of a device in a network by attaching a unique but mostly temporary number to it.[125] The IP addresses assigned to any electronic device in a computer network allow the transmission of data between devices. The three jurisdictions do not share a common understanding of how and when IP addresses should be classified as personal data, as will be shown in this section.

A. Australian Approach

In *Telstra* AAT, the Administrative Appeals Tribunal ruled "that an IP address is not information about an individual".[126] The AAT expressed the view that IP addresses, where they change regularly over the life of the respective device, only identify the respective device itself but are not information "about" the user of the device, because any connection

125. Information Sciences Institute, *Internet Protocol: DARPA Internet Program Protocol Specification*, University of Southern California Working Paper, RFC 791 (Marina del Rey, California: University of Southern California, 1981) at 5–10.

126. *Telstra* AAT, *supra* note 19 at para 113.

between the IP address and the user would be "ephemeral".[127] As the AAT put it, such IP addresses are "not about the person but about the means by which data is transmitted from a person's mobile device over the internet", and, therefore, they are not considered to be personal information under Australia's privacy regime.[128]

While the Federal Court of Australia upheld the decision of the AAT, the appeal was limited to the interpretation of the definition of "personal information", not its application. The Full Court merely held that the words "about an individual" had meaning and required consideration before the subsequent issue arose of whether this information identified that individual.[129] The Federal Court declined to consider whether the AAT applied its definition correctly because this was not raised in the appeal.[130] The Privacy Commissioner decided not to challenge the Full Court decision any further.[131] In its updated guidance on the meaning of "personal information", the issue of IP addresses is not covered.

However, another recent decision of the AAT, issued after the Full Court decision,[132] specifically adopts the reasoning of *Telstra* AAT. In *Freelancer International Pty Ltd and Australian Information Commissioner*, Freelancer operated a website that required user registration and a login by registered users. Freelancer recorded the login IP addresses and associated these IP addresses with particular registrant accounts, including by displaying the IP address used in a session in a Welcome message to the registrant. Nonetheless, the AAT held that while a user's identity might reasonably be ascertained from the information available to the website operator, the IP address information was "not "about" an invidual. It was information "about" the login itself".[133] Like *Telstra*

127. *Ibid*.
128. *Ibid*.
129. *Telstra* FCAFC*, supra* note 2 at paras 62–65.
130. *Ibid* at para 65.
131. Austl, Commonwealth, Office of the Australian Information Commissioner, *Statement on Privacy Commissioner v Telstra Corporation Limited Federal Court decision* (OAIC, 2017).
132. *Freelancer International Pty Ltd and Australian Information Commissioner*, [2017] AATA 2426.
133. *Ibid* at para 69.

AAT, this decision appears to assume that when information, such as an IP address, is about enabling a communication, it cannot also be about the individual engaged in that communication. This is in contrast to the decision of the Full Court, which did not subscribe to the view that the classification task is binary and stated specifically that information can have more than one subject matter.

In summary, while decisions of the AAT, both before and after *Telstra* FCAFC, suggest that IP addresses of electronic devices do not qualify as "personal information" and, hence, are not subject to Australian privacy legislation, these decisions are not completely free from doubt and potentially open to challenge.

B. Canadian Approach

As pointed out above, the Canadian definition of personal information resembles the Australian approach. Nonetheless, its application in practice appears to differ.

The Privacy Commissioner of Canada outlined that IP addresses do not only constitute the technical base for electronic communication but also provide a potential starting point to unlock additional information about the individual who used the electronic device which identified itself via the IP address in question.[134] A study conducted by the Canadian Privacy Commissioner showed that an IP address enabled the creation of a detailed profile of the device user including the geolocation of the user and other web activities as well as e-mail addresses from the user.[135] Therefore, the Canadian Privacy Commissioner classified IP addresses as being sufficiently linked to the individual using them and, therefore,

134. Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013), online: OPC < https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/>.

135. *Ibid*.

qualified them as personal information under Canadian law.[136] The decision of the Supreme Court of Canada in *R v Spencer*[137] provides further illustration of the link between an IP address and an identifiable user. In that decision, the Court decided that internet users may have a reasonable expectation of privacy over their internet activities and that a warrantless police request that an ISP provided identifying information about a subscriber of a particular IP address amounted to an unlawful search and violated the user's section 8 *Charter* rights.[138] Justice Cromwell, writing for the Court, further considered the application of the *PIPEDA* to subscriber information.[139] His Lordship concluded that there was a reasonable expectation of privacy in the subscriber information as the disclosure of such information "will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous" and, therefore, a request by a government institution to reveal this information "amounts to a search".[140]

C. European Approach

Under European Union data protection law, IP addresses normally fall within the scope of personal data. In 2011, the ECJ ruled in *Scarlet Extended* that IP addresses may allow the precise identification of the

136. Office of the Privacy Commissioner of Canada, "Metadata and Privacy: A Technical and Legal Overview" (October 2014), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/>; Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2001-25" (20 November 2001), online: OPC < https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/pipeda-2001-025/>. See also Eloïse Gratton, "Personalization, Analytics, and Sponsored Services: The Challenges of Applying PIPEDA to Online Tracking and Profiling Activities" (2010) 8:2 Canadian Journal of Law & Technology 299 at 300–05.
137. *R v Spencer*, 2014 SCC 43 [*Spencer*].
138. *Charter*, *supra* note 61, s 8.
139. *Spencer*, *supra* note 137 at paras 52 *et seq*.
140. *Ibid* at para 66.

persons using the addresses and, therefore, qualify as personal data.[141] This ruling adopted the opinion delivered by the European Advocate General, which expressed the view that an IP address "may be classified as personal data inasmuch as it may allow a person to be identified by reference to an identification number or any other information specific to him".[142] However, the decision in *Scarlet Extended* related to the introduction of a system for filtering electronic communications by the ISPs and, therefore, by entities which not only had access to IP addresses but — being the provider — also to the necessary data to link the IP addresses with specific users of the service.

The ECJ later expanded this view to IP addresses held by entities other than the ISPs. In *Breyer*, the ECJ stated that the notion of personal data in Article 2(a) of the DPD does not necessarily require that the data on its own allow the data subject to be identified or that the controller of the data must be able to identify the data subject without the help of a third party.[143] Instead, the ECJ ruled that it is sufficient if the data controller in question "has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority" and other private entities.[144] This criterion is fulfilled if the data controller "has the *legal means* which enable it to identify the data subject with additional data"[145] held by third parties, as long as this does not require "a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[146] The ECJ then applied this test to dynamic IP addresses stored by a website operator and came to the conclusion that such addresses allow the identification of the respective device connecting to the internet under the IP address in question because website operators may gain the necessary additional data from the competent authority

141. *Scarlet Extended*, *supra* note 46 at para 51.
142. EC, *Opinion of Advocate General Cruz Villalón delivered on 14 April 2011*, 2011:255 at paras 74–78.
143. *Breyer*, *supra* note 46 at paras 41 *et seq*.
144. *Ibid* at para 48.
145. *Ibid* at para 49 [emphasis added].
146. *Ibid* at para 46.

or the respective ISP. The ECJ finally concluded that under these circumstances, dynamic IP addresses constitute personal data within the meaning of Article 2(a) of the Data Protection Directive.[147]

This finding by the ECJ was met with approval among European scholars[148] so that the qualification of IP addresses as personal data under European Union law is no longer in serious doubt. As the definition of personal data in the *GDPR* remained virtually unchanged from the definition given by the DPD, the findings by the ECJ must be taken to remain applicable under the *GDPR*.[149] In the recent decision of *Benedik v Slovenia*,[150] the European Court of Human Rights held that subscriber information associated with a dynamic IP address fell within the scope of protection of Article 8 (right to private life) of the European Convention on Human Rights. In doing so, the Court adopted the jurisprudence of the ECJ in the *Scarlet Extended* and *Breyer* decisions and also specifically referred to the factually similar decision of the Canadian Supreme Court in *Spencer*.[151]

IV. Conclusion

Despite employing similar definitions of personal data or personal information in their data protection laws, these terms have been interpreted differently by courts in Australia, Canada and the European Union. Part of these differences may also be due to the fact that the courts across these jurisdictions differ in their willingness to consider international materials in their decisions. As a result, the scope of application of the

147. *Ibid* at para 49.

148. *Cf.* Schild, *supra* note 105 at para 19; Heiko Richter, "Datenschutzrecht: Speicherung von IP-Adressen beim Besuch einer Website" (2016) 27:23 Europäische Zeitschrift für Wirtschaftsrecht 912 at 913; Frederik Zuiderveen Borgesius, "The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition" (2017) 3:1 European Data Protection Law Review 130 at 135. This is in line with the prevailing view in legal literature before the ECJ judgments.

149. Borgesius, *ibid* at 136.

150. *Benedik v Slovenia*, No 62357/14 (24 April 2018).

151. *Scarlet Extended*, *supra* note 46; *Breyer*, *supra* note 46; *Spencer*, *supra* note 137.

respective data protection legislation does not coincide. This has the potential to create friction between these jurisdictions by forming an obstacle to the free flow of personal data as most countries only allow the export of personal data to third jurisdictions if an adequate level of protection is guaranteed. If one country establishes a narrower term of personal data than other countries, thereby constraining the scope of its data protection legislation, the export of such data into this country can become problematic. The lack of uniformity has been demonstrated by the example of IP addresses, which Australian law treats differently to Canada and the European Union..

The lack of harmonised interpretation could be addressed if the jurisdictions put more effort into creating alignment between the legal definitions they employ. Initial approaches exist, such as the *Convention 108*, which aims to create a common framework of data protection for its participating countries.[152] Even apart from international treaties, there are also inherent connections between the different jurisdictions. As shown above, the Canadian *PIPEDA* was enacted also against the background of the European data protection legislation and utilized its formulations. Australian case law, in turn, has made some limited references to a Canadian decision in support of its interpretation of Australia's data protection laws. However, against the background of increasingly global data flows, the time has come to develop these connections more systematically and, as the European Court on Human Rights has done in *Benedik*, to adopt a comparative approach to interpreting the key terms of data protection laws wherever possible.

152. *Convention 108*, *supra* note 103.

Canadian Journal of Comparative and Contemporary Law

Volume 4 | Number 1 | 2018

Privacy, Identity, and Control: Emerging Issues in Data Protection

Foreword
Justice Rosalie Silberman Abella
Supreme Court of Canada

Articles

Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression
Fiona Brimblecombe & Gavin Phillipson

Equality at Stake: Connecting the Privacy/Vulnerability Cycle to the Debate about Publicly Accessible Online Court Records
Jacquelyn Burkell & Jane Bailey

Privacy by Design by Regulation: The Case Study of Ontario
Avner Levin

Abandoning The "High Offensiveness" Privacy Test
N.A. Moreham

Regulating Surveillance: Suggestions for a Possible Way Forward
Moira Paterson

"A Virtual 'Puppet'": Performance and Privacy in the Digital Age
Megan Richardson

Information Brokers, Fairness, and Privacy in Publicly Accessible Information
Andrea Slane

When is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws
Normann Witzleb & Julian Wagner