Losing the Battle but Winning the War: Why Online Information Should Be a Prohibited Ground

*Avner Levin**

This paper contends that in the "war" to protect the privacy of individuals' personal information online, the battle to limit the collection of such information has been lost. Existing personal information protection regimes, with their emphasis on notice and consent, have proven inadequate, especially in light of the advent of "big data analytics" and revelations of large-scale privacy violations by governments and corporations. The author argues, however, that the war can still be won on another front — that of limiting the use of personal information. In developing this theme, the author explores the notion of "network privacy," which posits that information shared online within a given social circle is intended to stay within that social circle, and is not to be shared beyond its boundaries without permission. Currently there is no legal protection in Canada against the invasion of network privacy (though in several recent decisions, the courts have shown a more nuanced understanding of privacy in online information). One potential source of such protection might be the adoption of the "Oxford principles" formulated in 2013, which propose a new model for regulating the processing of information, one that is focused on the use of personal information rather than on its collection. In the author's view, though, those principles, as well as other proposals, would not provide sufficient protection. Instead, the author outlines an approach that is broadly similar to the prohibition against the use of information relating to protected grounds under Canadian human rights legislation. Under this approach, no action could be taken against an individual — including in the employment context — based on his or her online information, except where that information reveals criminal, illegal or unethical conduct, or causes significant harm to others.

1. INTRODUCTION

Although the topic of this paper is privacy in the workplace, it has inevitably been shaped by the revelations of government electronic surveillance conducted by the United States and several of its

* Associate Professor and Director, Privacy Institute, Ryerson University.

allies,[1] and (to a lesser extent) of corporate surveillance and breaches of privacy. The revelations about the magnitude of the American National Security Agency's (NSA) surveillance programs dwarf the more mundane workplace privacy concerns typically raised by employees and their union representatives.

Ironically, around the same time that news broke about the NSA, the Organisation for Economic Co-operation and Development (OECD) was putting the finishing touches on the first revision to its data protection principles in thirty years.[2] The revised guidelines were formally adopted in July 2013, one month after the first information about the NSA was revealed. The guidelines understandably represented the end of a long process and could not possibly serve as a reaction to the new information.[3] The main new concepts that the guidelines incorporated were: mandatory data breach notification, organizational privacy management programs, and national privacy strategies.[4] And the timing of their adoption presented an opportunity to call for more radical revisions.

Around the same time, early in 2013, the Oxford Internet Institute organized a workshop that produced a white paper entitled *Data Protection Principles for the 21st Century* ("Oxford principles").[5] The proposed principles were meant to address the privacy

---

1 There have been many news reports of these programs since the summer of 2013. The original story broke in *The Guardian*, and that newspaper currently maintains a comprehensive website about the United States' surveillance. See "The NSA Files," *The Guardian*, online: <http://www.theguardian.com/world/the-nsa-files>.

2 For information on the OECD process, see Internet Economy, *OECD work on privacy*, online: OECD <http://www.oecd.org/sti/ieconomy/privacy.htm>.

3 The guidelines were created through the work of the OECD's privacy expert group. See OECD, *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines*, OECD Digital Economy Papers No 229 (OECD, 2013), online: <http://dx.doi.org/10.1787/5k3xz5zmj2mx-en>.

4 For the revised guidelines in full, see OECD, *OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data* (2013), online: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.

5 See Fred H Cate, Peter Cullen & Viktor Mayer-Schönberger, "Data Protection Principles for the 21st Century" (Report delivered at a drafting workshop hosted by the Oxford Internet Institute, January 2013), online: <http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf>.

concerns around "big data" and were not based on the NSA revelations.[6] Nonetheless, they offer an interesting response to the challenge posed to the principles of data protection by widespread surveillance and information collection. The Oxford workshop viewed the notice and consent model at the heart of existing data protection legislation as unable to cope with the challenges posed by big data analytics.[7] In order to compensate for this perceived weakness, the white paper places increased responsibility on data collectors and users of data. It also strengthens the principles that govern and restrict data use.[8] The Oxford principles have been the subject of some controversy and perhaps misinterpretation since their release in late 2013.[9]

This paper argues that one of the lessons already learned from the NSA revelations is that the valiant battle to limit the collection of personal information online is lost, and has been lost for some time. Limiting the collection of personal information is one of the principles at the heart of Canada's personal information legislation. Therefore, such an argument is disheartening, to say the least.[10] However, this paper contends that the "war" over privacy, if such a term can be used, can be fought and hopefully won over another fundamental principle — that of limiting the use of personal information.[11]

The principle of limited use should be strengthened and upgraded, so that in some circumstances the use of personal information obtained from online sources will be prohibited outright. This

---

6 "Big data" is the popular term for the extremely large amounts of information collected for commercial purposes. Sophisticated analytical algorithms, yet to be developed, are supposed to unlock the insights that exist within these data sets.

7 Cate, Cullen & Mayer-Schönberger, *supra* note 5 at 6-7. Notice and consent are two data protection principles that require data collectors to notify individuals before their information is collected, or to obtain consent from individuals prior to such collection. Whether notice or consent is required depends on the jurisdiction and circumstances of collection.

8 *Ibid* at 8.

9 See e.g. Ann Cavoukian, "So glad you didn't say that! A response to Viktor Mayer-Schönberger" (16 January 2014), *International Association of Privacy Professionals* (blog), online: <http://www.privacyassociation.org/news/a/so-glad-you-didnt-say-that-a-response-to-viktor-mayer-schoenberger/>.

10 *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5, Schedule 1, s 4.4 [*PIPEDA*].

11 *Ibid* at Schedule 1, s 4.5.

could be done in a way similar to that in which certain personal information collected off-line, such as information about an employee's (or a job applicant's) race or gender, is prohibited. The framework of "prohibited grounds" established by the federal and provincial human right codes and supported by the *Canadian Charter of Rights and Freedoms* governs, among other things, the job application process and the ongoing employment relationship. This framework should be transposed onto privacy law to protect the privacy interests that individuals have in online information, just as human rights laws protect individuals against the use of information that they inevitably share about their race, gender or other protected personal characteristics. The employment relationship might serve as the prototype for protection of privacy online more generally. This is a fitting role, perhaps, given the dismal and enabling role employers and corporations more generally have played in the erosion of privacy.[12]

To make the argument that online information should, in certain circumstances, be treated similarly to prohibited grounds information, this paper proceeds as follows. First, the paper discusses the notion of online privacy, why personal information available online deserves protection, and the implications for the employment relationship and the ability of the employer to make use of such information.[13] Second, the paper briefly reviews the Canadian legal framework protecting employees and Canadians generally from discrimination — the "prohibited grounds" framework. Third, the paper considers alternative approaches to the protection of privacy in online information, with a particular focus on the revised data protection principles proposed by the Oxford workshop and their applicability to workplace privacy. Finally, the paper suggests how the "prohibited grounds" model could apply to online information, and the circumstances in which online information should be treated as if it were "prohibited grounds" information. It then demonstrates the utility of this treatment through a

12 Avner Levin, "Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada" (2007) 22:2 CJLS 197.

13 This section builds upon the work done by the author and his colleagues. See Patricia Sánchez Abril, Avner Levin & Alissa Del Riego, "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee" (2012) 49:1 Am Bus LJ 63 [Abril, Levin & Del Riego].

few examples. In the end, the paper offers a normative argument for the crucial, future development of the idea of privacy online.

2. THE NOTION OF PRIVACY ONLINE

One of the unfortunate, and perhaps unexpected, consequences of our increased activity online through social media and through the generation of personal "content" has been the emergence of a common wisdom that information available online is "public" and thus fair game for employers, government, friends and adversaries. For example, in one of the early social media litigation cases in Ontario, the Court opined that "the plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site."[14] In fact, research demonstrates that participants and users of social media have strong privacy expectations. However, the law has yet to acknowledge these expectations.[15]

My colleagues and I have referred elsewhere to these expectations of privacy online as a notion of "network privacy."[16] Network privacy protects the need of individuals to create their identity and their persona online. If such protection did not exist in the offline world, we would not be able to engage in the forms of identity formation that we take for granted, and that sociologists, such as Goffman, have argued are essential for societal interaction.[17] Importantly, identity formation requires a considerable amount of information-sharing to create the perception of an identity in the minds of others, or in Goffman's terms, in the minds of the "intended audience."[18] In the real world, it is fairly easy — although not always completely possible, thanks to long-held and well-established social norms — to

---

14 *Murphy v Perger* (2007), 67 CPC (6th) 245 at para 20 (Ont Sup Ct J) [*Murphy*].

15 I discuss some promising recent production decisions in the section titled Canadian Privacy Jurisprudence, below. See generally (for the discrepancy between the expectations of social media users and the law with regards to privacy) Avner Levin & Patricia Sánchez Abril, "Two Notions of Privacy Online" (2009) 11:4 Vand J Ent & Tech L 1001 [Levin & Abril].

16 *Ibid* at 1045.

17 Erving Goffman, *The Presentation of Self in Everyday Life* (Garden City, NY: Anchor Books, 1959).

18 *Ibid* at 49.

control the manner in which this information is shared. It is also possible to share different information with various audiences, leading ultimately to the creation of distinct personas, such as an individual's professional identity, religious identity, social identity and others. In the context of the workplace and the employment relationship, it is this ability to project different personas to different audiences that we seek to protect by insisting on some separation between work and private life.

However, due to the permanency of digital records online, and the ease of their dissemination, the separation of our information to support distinct identities becomes much more difficult. It is all the more so due to the social nature of this particular information — information that is not intended to be secluded or protected, but shared and used to construct an identity. Online social networks, as opposed to real-world social networks, pose an additional challenge since they are often larger and not based exclusively on real-world connections. It is this technological challenge to identity, dignity, reputation and image that network privacy seeks to counter, just as intellectual property seeks to counter the ease with which technology enables the infringement of copyright and other intellectual property rights.

Network privacy is the notion that harm warranting a remedy occurs when information is shared indiscriminately across social network boundaries, for example, when so-called friends of an employee transfer compromising information to an employer.[19] According to network privacy, information shared with a specific social circle is intended to remain within that social circle. That individual places implicit confidence and trust in other members of the social circle. He or she does not intend the information to be shared outside the boundaries of that social circle without their control and permission. An employee, for example, may wish to complain about her manager, or her customers, to her friends, but will not want the manager or the customers to have access to her posts or tweets.[20]

---

19 See Lior Jacob Strahilevitz, "A Social Networks Theory of Privacy" (2005) 72 U Chicago L Rev 919 at 974-975. See generally, Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2009).

20 See e.g. Eric Frazier, "Facebook post costs waitress her job," *The Charlotte Observer* (17 May 2010), online: <http://www.charlotteobserver.com>.

It is important to note that the employee, and individuals more generally, will not wish information to be shared *only* because of concerns over real-world negative implications, such as discipline or termination of employment. Individuals want to completely control the context in which their information is presented, so that they can develop their respective identities and personas. An employee may simply wish to present herself as professional, diligent and loyal to her supervisors, and as a result, construct her workplace persona and identity to fit such values.

Legal recognition of network privacy would recognize as a basis for legal action the sense of harm experienced by individuals when their information is shared unwillingly across social boundaries online. This would entitle individuals to a legal remedy. Of course, the law would not want to prohibit *every* form of information-sharing that could be considered a breach of network privacy. I discuss below the factors that would be required to prohibit such information-sharing, or more accurately, to prohibit the *use* of information obtained through breaches of network privacy.

Interestingly, research demonstrates that in the absence of legal and social norms, practices of "netiquette" are created to support network privacy.[21] The development of such "netiquette" is also an indication that the privacy policies and tools put in place by the corporations that provide social media are inadequate. To the extent that they exist, such tools focus on the handling of personal information by the social media operator and its affiliates, not on the sharing of information between the individuals that socialize online. This is unfortunate, since social media corporations are best positioned to develop effective tools and policies to protect network privacy.[22] One example of evolving online social norms involves photo-tagging among teens; the current norm is that identifying photos should be removed at the request of the individuals who appear in them.[23] What the protection network privacy provides, if respected, is the protection of the sense of self, identity and of reputation and dignity. It is entwined with the

---

21 Jacquelyn A Burkell *et al*, "The View From Here: User-Centered Perspectives on Social Network Privacy" (2013) FIMS Library & Information Science Publications 25, online: <ir.lib.uwo.ca/fimspub/25>.

22 Levin & Abril, *supra* note 15 at 1047.

23 Burkell *et al*, *supra* note 21 at 14-15.

formation of all of these notions, especially, but not exclusively, in the case of teens and young adults. Unsurprisingly, perhaps, while individuals prefer that their privacy online enjoy some protection, they almost always opt for the ability to create and influence their persona through online activities, over the supposed alternative of withdrawal from participation in social media.[24]

Focusing on the formation and protection of identity and self, it is clearer why a notion of online privacy that is based on social networks — network privacy — exists. Importantly, it becomes apparent why it is possible for individuals to have an expectation of privacy online despite the common fallacy of setting expectations of privacy by the number of individuals who have access to information. Since online privacy focuses on the control of information as it is shared across social networks, it is not concerned with the question "how many people know," but with "*who* knows." Common arguments for dismissing privacy expectations, such as those referencing numbers of "Twitter Followers" or "Facebook Friends" as an indication that no privacy expectation exists, are irrelevant to network privacy. A sense of privacy online can co-exist with access to Facebook information by hundreds of friends, and instantly disappear when just one other individual — the boss — is informed.

Individuals attempt to protect themselves from negative consequences at work arising from the disclosure of personal information they post online. Privacy is often the reason provided for why employers should not be given access to information, or prevented from acting upon information that somehow came to their attention. Data demonstrate that while employees are happy to use social media to advance up the corporate ladder, they are quite adamant about maintaining as strong a separation as possible between their personal and work lives.[25] Thus, employees generally agree that access to social media should be prohibited during work hours or on work devices. This desire to separate work from private life is of course a manifestation of a desire for network privacy. However, the paucity of clear employer policies regarding online conduct, at work and when not working, does not promote the realization of such a separation.[26]

---

24 Levin & Abril, *supra* note 15 at 1046.

25 Abril, Levin & Del Riego, *supra* note 13 at 103.

26 *Ibid* at 105.

Network privacy is important not only to workers. Applicants, as individuals who wish to present their best professional persona in order to secure employment, have a strong expectation of network privacy.[27] Applicants do not wish to forgo participation in social media in order to gain employment. They wish to share information selectively, but truthfully, on social media to protect their image and identity.

However, the online behaviour of individuals is somewhat paradoxical. Individuals desire network privacy, while sharing a fair bit of information online that could quite probably cause them harm. I argue below that the solution to this ostensible paradox can be modelled on other situations in which individuals share information and information is collected about them — not necessarily with their consent and approval — and in which harmful action on the basis of this information is nevertheless prohibited by law. Those circumstances exist with respect to information about individuals such as their sex, colour, age and other protected characteristics. Those characteristics, by law, cannot form the basis of action against the individuals, and such action would constitute prohibited discrimination. The next section provides a brief review of the prohibited grounds framework in Canada. The paper then turns to the application of this model to online information.

3. THE PROHIBITED GROUNDS FRAMEWORK IN CANADIAN HUMAN RIGHTS LAW

One publicly accepted model of limiting action on the basis of widely available information is the prohibited grounds model. Members of Canadian society are prohibited from acting against individuals in prescribed circumstances on the basis of prohibited grounds, which are listed in our federal and provincial human rights codes.[28] These are substantive grounds upon which discrimination is prohibited, such as an individual's sex, colour or religion. Individuals have a right to expect that decisions will not be made against them

27 *Ibid* at 108.

28 See e.g. *Canadian Human Rights Act*, RSC 1985, c H-6, s 3 [*CHRA*]. The differences across Canada between the legal protection of human rights do not affect the argument of this paper.

on the basis of a prohibited ground, although the legislation provides for certain exceptions (for historical reasons as well as reasons that reflect contemporary social mores).[29]

The right to equal treatment is not limited to the workplace. It extends to other social interactions such as contractual transactions, the receipt of goods and services, the use of facilities, housing decisions, and membership in associations and unions.[30] Thus, the discussion in this paper of the potential of the prohibited grounds model to inform the use of online information is not necessarily limited to the employment relationship. Importantly, the prohibited grounds model applies to decisions about employment (i.e. hiring and firing) as well as to decisions made while the employment relationship subsists (e.g. promotion and discipline).[31] Job applicants are particularly vulnerable to discrimination, and so a model that applies to their information and that could be extended to online information (increasingly the basis for hiring decisions) is potentially quite useful.[32]

There are of course many ways in which discrimination can take place. It can take the form of harassment, systemic discrimination or a poisoned work environment. It can be in response to association with a person, or arise out of a failure to act inclusively.[33] Regardless of form, examined from the perspective of personal information protection principles, discrimination is properly understood as use of information for a forbidden purpose. Of course, the act of collecting personal information can be itself discriminatory or lead to a strong

---

29 For example, religious, educational and several others institutions are allowed to hire individuals on the basis of prohibited grounds — such as religion or physical disability — if the purpose of the institution is to serve the specific group of people that share the same prohibited ground. See *Human Rights Code*, RSO 1990, H.19, s 24 [*HRC*].

30 *Ibid* at Part I.

31 *Ibid* at s 23. See also Ontario Human Rights Commission, *Human Rights at Work*, 3d ed (Toronto: Carswell, 2008) at ch 3, s 1 [OHRC].

32 Newly proposed amendments to the federal private-sector personal information protection statute recognize the utility of this model by extending whatever protection that statute offers to applicants for employment as well. See Bill S-4, *An Act to Amend the Personal Information Protection and Electronic Documents Act and to Make a Consequential Amendment to Another Act*, 2d Sess, 41st Parl, 2014, cl 3 (first reading 8 April 2014) [*Digital Privacy Act*].

33 OHRC, *supra* note 31 at ch 3, s 2.

likelihood that discrimination will occur. That is why human rights codes specify that discrimination occurs when job applicant information is collected on the basis of one of the prohibited grounds.[34]

Indeed, Ontario Human Rights Commission guidelines include detailed instructions regarding permissible collection on application forms, as well as permissible collection during interviews.[35] By and large, overt information collection is prohibited. But the collection of personal information on many of the prohibited grounds is inadvertent and unavoidable. Consider the full list of prohibited grounds with respect to employment in the province of Ontario: race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, gender identity, gender expression, age, record of offences, marital status, family status or disability.[36] Of these, race, colour, sex, age and disability are arguably immediately "collected" at the first instance of human interaction — for example, at the interview stage. Others — such as ancestry, place of origin and ethnic origin — are then inferred from the person's dialect, accent and personal conduct as the interaction continues. Still others are easily assumed, such as creed, sexual orientation, gender identity and gender expression, which can often be gathered from a person's clothes and external appearance. In short, it is possible to inadvertently "collect" almost all of the personal information which relates to prohibited grounds under human rights legislation.

While the collection of personal information relating to prohibited grounds is not condoned, the principles at the basis of the prohibited grounds model focus on the prohibition of discriminatory use. These principles recognize, as a practical matter, that personal information may well be "collected" despite the best intentions of employer and applicant. Employers are instructed, therefore, not to act discriminatorily on the basis of the personal information that they hold about applicants. That is the gist of the prohibited grounds approach to human rights (in the context of employment).

Every model has its exceptions, and if the model of prohibited grounds is to be adapted for the purposes of protecting

---

34 *CHRA*, *supra* note 28 at s 23.

35 OHRC, *supra* note 31 at ch 4, s 4-5.

36 *CHRA*, *supra* note 28 at s 5.

online informational privacy, it is worthwhile to inquire into those exceptions, and in particular into the basis for permitting the use of prohibited information. The principles that guide these exceptions may serve as building-blocks to guide situations in which the use of information collected online would be permissible as well. One well-known exception, operating by way of a defence to claims of discrimination, is that employment requirements may adversely impact individuals on the basis of protected personal characteristics if they are "*bona fide*," i.e. rationally connected to the job, adopted in good faith, and reasonably necessary.[37] I discuss below how the same essential principles can be applied to the use of online personal information. There should be a rational connection between information and proposed use, good-faith conduct by the employer, and reasonable necessity. A balancing of interests plays a role in formulating the rules for use of personal information that originated online. The Oxford principles, which I discuss in the next section, are in a similar vein. They propose that the protection of personal information should focus on the use of such information, not on its collection. I will consider why those principles, along with other proposals such as the formalization of the collection and use of online information, are not adequate to ensure that such a balancing of interests takes place.

4. THE OXFORD PRINCIPLES

The Oxford principles are an attempt to formulate "Data Protection Principles for the 21st Century."[38] The proposal for revised OECD guidelines was meant to address the changes that have occurred in data processing from the late 1970s and early 1980s to the present day, with particular focus on the challenges of "big data" analytics.[39] The proposal points out many of the commonly accepted flaws in the way that current data protection regimes work, such as privacy policies that individuals do not bother to read, or terms of use to which individuals "agree" with the click of a mouse.[40] These

37 This is a summary of the well-known *Meiorin* test. *British Columbia (Public Service Employee Relations Commission) v BCGEU*, [1999] 3 SCR 3 at para 54, [1999] 10 WWR 1.

38 Cate, Cullen & Mayer-Schönberger, *supra* note 5.

39 *Ibid* at 5-6.

40 *Ibid* at 6-7.

were meant originally to provide individuals with notice about the ways in which their personal information will be collected and used, and in certain jurisdictions, to obtain the consent of individuals for such information practices. The original purpose of principles such as notice and consent was to provide individuals with control over their personal information. The reality in the last decade has been an erosion of control, with privacy policies and "click-wrap" agreements serving to whitewash questionable information practices.[41]

The proposal, mindful of the many positive implications of big data analytics, attempts to restore the balance between individual data subject and organizational data processor.[42] The proposal is the culmination of several workshops in 2012 and 2013. Released late in 2013, it represents the joint work of academics, and former data protection regulators and industry professionals.

The stated goal of the group, as mentioned above, was to shift responsibility for the protection of personal information from the shoulders of individuals to the organizations that process the information.[43] The proposal attempts to achieve that goal by moving away from the discredited notice- and consent-based model to a model focussed on permissible use. At the heart of the proposal stand a revised set of data principles and accompanying revised definitions of concepts related to personal information.[44]

The proposal refers to all data-related activity as information processing.[45] Within processing, four categories are proposed — information collection, use, storage and destruction.[46] Significantly, the proposal suggests that the existing category of disclosure (of information to third parties) be eliminated in order to facilitate both the movement of data and the accountability of organizations.[47] Accordingly, the use of information is defined in the proposal to cover the following activities: the reliance on personal information for decisions about, or assessments of, individuals; the creation or inference

41 *Ibid*.
42 *Ibid* at 8.
43 *Ibid* at 11.
44 *Ibid* at 14-21.
45 *Ibid* at 15.
46 *Ibid*.
47 *Ibid*.

of more personal information; and the disclosure or dissemination of personal information to others.[48]

Of the eight principles suggested in the proposal, one addresses information collection, three address information use (as newly-defined), and four address information processing in general. The information *collection principle* dispenses with the existing requirements of notice or consent for collection. Instead, it allows for information collection as long as the information is not collected in violation of the law, through deception or in hidden ways.[49] It is this revision, the elimination of the requirement of consent to collection, which has drawn the most attention from critics.[50] The revision reflects the sense that the battle over the collection of personal information has been lost, and that undue focus on notice and consent requirements has resulted in technical but not meaningful privacy protection regimes.[51] In light of Edward Snowden's revelations on the NSA, it is worth noting that the collection principle does address government collection, which is prohibited unless the collection is based on legal authority or has a legitimate purpose.[52]

The manner in which the war over privacy could yet be won is described by the proposal's *use principle*. Rather than list permissible uses (and acknowledging that such listing would be a futile exercise), the proposal suggests that use of personal information should be allowed if the benefits of use outweigh the harm of use.[53] The proposal defines harm as encompassing both tangible and intangible harm (e.g. the feeling of an invasion of privacy). However, it excludes from the definition of harm any negative results of the "appropriate" application of personal information to an individual, an important matter to which I will return.[54]

---

48 *Ibid*.

49 *Ibid* at 15-16.

50 Cavoukian, *supra* note 9.

51 Cate, Cullen & Mayer-Schönberger, *supra* note 5 at 16.

52 *Ibid* at 15. Of course, proponents of the NSA programs have argued for their legitimacy.

53 *Ibid* at 17-18. Benefits could be to the individual, to others or to society at large.

54 *Ibid* at 14. The proposal does not elaborate on the meaning of "appropriate" application. Presumably the definition is intended to curtail claims of harm arising out of routine commercial transactions. If that is the case, it is an unfortunate concession to commercial interests.

Once the balancing of benefits and harms has commenced, the proposal suggests that use involving no harm, or minimal harm, should be allowed and that use resulting in significant harm (e.g. personal injury) should be prohibited. Use that falls in the middle ground should be allowed, as long as appropriate protection is in place.[55] One of the ways in which appropriate protection could be secured is through the provision, at this stage, of individual consent. However, the proposal states that such consent, or individual choice, must be meaningful, real and informed.[56] It is questionable whether such consent can exist in the context of an employment relationship or of an application for employment.[57]

The proposal includes two other use-related principles, one to ensure the quality of personal information (the *quality principle*) and the other to allow for individual access to his or her personal information, titled the *individual participation principle*. This second principle provides individuals with the opportunity to access their personal information and to challenge its accuracy and the ways in which it is processed.[58] However, this right of access is provided only when the use of personal information has an impact on the individual's education, employment, health or finances, or other legal right of the individual.[59]

Of the four principles that address information processing in general, two that are largely unchanged (the *openness principle* and

---

55 *Ibid* at 17.

56 *Ibid*.

57 Telus sought employee consent for voice recognition identification. Employees were informed that refusal to consent may result in progressive discipline. The Court ruled that, while threats of disciplinary measures normally vitiate consent, informing employees of potential consequences does not amount to such a threat. Furthermore, disciplining employees for refusing to provide consent would not be a breach of *PIPEDA*. The Court's decision illustrates the inherent difficulty of the application of the consent principle to the workplace. See *Turner v TELUS Communications Inc*, 2007 FCA 21 at paras 29-31, [2007] 4 FCR 368.

58 Cate, Cullen & Mayer-Schönberger *supra* note 5 at 18-19. Note that the principle does not guarantee that such challenges will be successful.

59 *Ibid* at 19. While the inclusion of the employment relationship (including potentially, an application for employment) is significant for the purposes of this paper, generally this principle prevents individuals from challenging and accessing their personal information if it is used for commercial purposes (such as the delivery of targeted ads).

the *security principle*) require organizations to be open about their information practices, and to secure personal information under their control.[60] The third, the *accountability principle*, essentially requires organizational compliance. It has been revised to include the consequences of non-compliance for organizations, in the form of liability for reasonably foreseeable harm.[61] The inclusion of legal liability within the principle is another tool that the proposal uses, in conjunction with the modified use and collection principles, to shift responsibility for data protection from individuals to organizations.[62] That is the tack taken in the eighth and final principle of the proposal, the *enforcement principle*. It is a new principle and requires the member states of the OECD to enforce these principles through national legislation, thus ensuring they will be taken into consideration by organizations that collect personal information.[63]

Taken in its entirety, the Oxford proposal suggests a new model for regulating the processing of information. This new model clearly distinguishes between information that can identify — and have a negative impact on — an individual, and information that cannot. It focuses on the former, and excludes the latter from its scope. Furthermore, the proposal suggests that information can be collected without notifying individuals or requiring their consent, and that meaningful restrictions on the processing of information should only be placed on the ways in which information is used. The elimination of the notice/consent requirement emanates not from a principled objection to these means of control, but rather from a concern that they have evolved over the years into a fig leaf that allows organizations to carry out unfettered processing on the pretext of individual agreement.[64] Instead of the requirements of notice and consent, the proposal suggests that organizations engage in harm/benefit analyses to determine whether specific uses of information should be allowed. Only uses that result in significant harm should be prohibited outright.

However, the proposal suggests that most uses will result in little harm, or in harm that could be mitigated by other means, and therefore

60 *Ibid* at 20.
61 *Ibid*.
62 *Ibid* at 21.
63 *Ibid*.
64 *Ibid* at 16.

that most uses would be allowed.[65] Importantly, it does not appear that decisions about employment — even termination — would be considered by the proposal's standards to cause significant harm to an individual, though the proposal acknowledges that such uses of information have a negative impact on individuals. There is a subtle distinction here between harm and impact. The proposal states that "harm does *not* include the rational and reasonable impact of accurate, relevant data appropriately applied to an individual."[66] Applying this definition to the workplace, it appears that should the use of personal data reveal employee conduct warranting dismissal for "just cause," such use by the employer would be considered, according to the proposal, "accurate" and "relevant," and its impact "rational."

How, then, would the principles of the proposal apply to workplace privacy issues? First, employers would be free to collect personal information about their employees. Notice to employees, or employee consent, would not be required.[67] In order to use the personal information that they have collected, employers would have to conduct a harm/benefit analysis.[68] If the outcome is little or no harm, the employer would be free to use that information. If the outcome is significant harm, the employer would be prohibited from using the information. Most analyses would result in an outcome that is in between these two extremes, and would require some form of protection. The use of personal information by employers could therefore depend on a privacy impact assessment (a tool familiar to privacy practitioners)[69] or perhaps on the agreement of employees. However, it is also possible that employers will argue that the use of personal information against employees, e.g. for disciplinary purposes, is

---

65 *Ibid* at 18.

66 *Ibid* at 14 [emphasis added].

67 *Personal Information Protection Act*, SA 2003, c P-6.5, s 15; *Personal Information Protection Act*, SBC 2003, c 63, s 13. In Canada, interestingly, the two provincial private-sector personal information statutes that govern workplace privacy (Alberta and British Columbia) do not require employee consent.

68 At the federal level, the private-sector data protection statute (*PIPEDA*) requires employee consent, but recent amendments proposed by the government dispense with that requirement. See *PIPEDA*, *supra* note 10 at Schedule 1, s 4.5; *Digital Privacy Act*, *supra* note 32 at cl 7.4.

69 See generally Office of the Privacy Commissioner of Canada, "Privacy Impact Assessments," online: <http://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp>.

"appropriate" and therefore, according to the definitions in the proposal, not harmful at all and not requiring a harm/benefit analysis.

In workplaces where employees are unionized, such ambiguities would doubtless become the subject of collective bargaining and/or to arbitral decisions. The determination of whether use is "appropriate" might end up resembling current discussions as to whether use is "reasonable."[70] Even if arbitrators found that workplace-related use is not "appropriate," employers would still be able to engage in the ensuing harm/benefit analysis and argue that the use should be permitted.

Of course, the majority of private-sector employees are not covered by a collective agreement and therefore do not have access to arbitration. In their situation, this preliminary and general analysis suggests that the Oxford proposal allows for the widespread processing of personal information with few restrictions. It is understandable why the cumulative effect of these increasingly narrow limitations has led some critics to question the efficacy of the proposal overall in achieving its stated purpose of better organizational protection of personal information.[71]

5. PROTECTING NETWORK PRIVACY

In Canada there is currently no legal protection against the invasion of network privacy.[72] With the promising exception of some recent procedural decisions that I discuss immediately below, courts have rejected arguments that information located on social networks is private and should not be disclosed. Information shared with a group of online friends has been treated by courts as public, the number of online friends often being cited in support for doing so.

---

70 See *PIPEDA*, *supra* note 10 at Schedule 1, s 5.3.

71 See e.g., Ann Cavoukian, Alexander Dix & Khaled El Emam, "The Unintended Consequences of Privacy Paternalism," *IPC Discussion Papers* (2014) [last accessed August 27 2014].

72 Canada, Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary on the Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) Against Facebook Inc. under the Personal Information Protection and Electronic Documents Act*, by Elizabeth Denham (Ottawa: Office of the Privacy Commissioner of Canada, 16 July 2009), online: <https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp>.

Courts have failed to consider that privacy online is contextual and network-specific.[73]

In workplace disciplinary proceedings, arbitrators have applied the same approach as the courts, ruling that Facebook posts are public and can be used by employers, since they were available to a number of people.[74] Such decisions fail to recognize the notion of network privacy, in either an empirical or a normative sense. Collection is indeed increasingly unfettered. Employers are looking up information on applicants with the aid of search engines, data brokers, friends of friends, and requirements that applicants hand over passwords and access to their social networking profiles.[75]

On the other hand, it may be that courts are beginning to develop a more nuanced understanding of privacy and information online. Two recent Ontario production decisions are worth discussing in some detail. They are procedural decisions on whether, in civil litigation, one party must produce the information demanded by the other party as part of the discovery process. In the first, the defendant in a civil lawsuit over a traffic accident requested that the plaintiff produce all of the vacation photographs she took after the accident, as well as all of her "private" Facebook account content.[76] The plaintiff argued that her Facebook account served as her digital photo album.[77] One hundred and thirty-nine Facebook friends had access to these photos and other content, which she considered private.[78] Based on the number of friends and earlier decisions, the Court could have easily ruled that

---

73 See *Murphy*, *supra* note 14. But see the recent decisions in *Stewart v Kempster*, 2012 ONSC 7236, 114 OR (3d) 151 [*Stewart*]; *Garacci v Ross*, 2013 ONSC 5627, 232 ACWS (3d) 341 [*Garacci*].

74 See *Lougheed Imports Ltd v UFCW, Local 1518* (2010), 186 CLRBR (2d) 82 (BCLRB) [*Lougheed*].

75 *Pietrylo v Hillstone*, 2008 WL 6085437 (DNJ 2008) [*Pietrylo*]; Neal Augenstein, "Maryland AG: Requiring Employees' Personal Passwords is Legal," *WTOP* (23 February 2011), online: <http://www.WTOP.com>.

76 See *Stewart*, *supra* note 73 at para 1.

77 *Lougheed*, *supra* note 744 at para 4.

78 *Ibid.*

the plaintiff had no reasonable expectation of privacy in the photos.[79] Significantly, however, the Court rejected that argument:

> To return to Murphy, Rady J. noted that the plaintiff in her case had 366 "friends" . . . and concluded that the plaintiff did not have a serious expectation of privacy . . . .
>
> The matter can, however, be viewed from the opposite direction. At present, Facebook has about one billion users. Out of those, *the plaintiff in the present case has permitted only 139 people to view her private content. That means that she has excluded roughly one billion people from doing so*, including the defendants. That supports, in my view, the conclusion that she has a real privacy interest in the content of her Facebook account.[80]

This articulation by the court of the plaintiff's privacy interest is the closest a court has come to-date to the recognition of network privacy as a legitimate interest that should be balanced against other interests in the judicial process. The Court recognized that the number of people who have access to information may not be as important as the attempt by an individual to determine *who* will have access to that information.[81]

The Court then considered the defendant's request to produce all of the other private Facebook account content. The Court had the following to say about this request:

> Before the dawn of the Internet age, people often communicated by writing personal letters to each other . . . . However, it is unimaginable that a defendant would have demanded that a plaintiff disclose copies of all personal letters written since the accident, in the hope that there might be some information contained therein relevant to the plaintiff's claim for non-pecuniary damages. *The shocking intrusiveness of such a request is obvious. The defendants' demand for disclosure of the entire contents of the plaintiff's Facebook account is the digital equivalent of doing so*.
>
> . . .

79 That was the analysis in cases such as *Murphy*, *supra* note 14.

80 *Stewart*, *supra* note 73 at paras 23-24 [emphasis added].

81 Admittedly, the courts still have some distance to go. A more critical reading of these paragraphs could conclude that just as the Court in *Murphy* found reason to argue that 366 was a high number, by comparing it to zero, so the Court in *Stewart* found reason to argue that 139 was a low number, by comparing it to one billion. Still, the contemplation that a person may have a privacy interest in information that is available to over one hundred people is noteworthy.

> The defendants' request to search the plaintiff's private correspondence and other data in her Facebook account in the hope that they might find something useful is akin to searching the plaintiff's filing cabinet. It is a fishing expedition and nothing more.[82]

The Court's recognition of a privacy interest in online information, and the analogy drawn by the Court between such information and written correspondence, are notable, given that privacy interests in real-world items, such as filing cabinets and garbage cans, have arguably been eroded.[83] In all events, this decision may represent a growing acceptance of the idea that there is privacy in online information, and that it deserves legal protection.

Indeed, a second recent decision appears to understand online privacy in this manner.[84] While the Court did not engage in an explicit privacy analysis, it endorsed the understanding of a Facebook account as a personal space, where individuals store personal information, such as photos, which they share with their friends (but not necessarily the public).[85] The litigation in that case concerned a traffic accident. The defendant again requested access to all of the photographs on the private section of the plaintiff's Facebook account — a request which the Court denied on the basis that it was nothing more than a "high-tech fishing expedition."[86] It is hoped that such decisions will lead to greater recognition and acceptance of the notion of privacy online, in the courts and at arbitration.

I discuss some American decisions related to network privacy below. However, the discussion in those decisions centers on personal health information and its attempted use by employers. Some of this information, such as employee medical and genetic information, is available online.[87] European-based attempts to mitigate the impact

---

82 *Stewart*, *supra* note 73 at paras 29, 31.

83 See also *infra* note 102.

84 *Garacci*, *supra* note 73.

85 *Ibid* at para 9.

86 *Ibid*.

87 See e.g. Heather Patterson, "Contextual Expectations of Privacy in Self-Generated Health Information Flows" (Paper delivered at the TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy, 30 March 2013), online: <http://www.ssrn.com/abstract=2242144>; Pauline Kim, "Medical Privacy, Anti-Discrimination Law and Employee Wellness Programs (Paper delivered at the Privacy, Law and the Contemporary Workplace: New Challenges and Directions, 22 November 2013) [unpublished].

of use of personal information derived from online sources have focused on the notion of control over that information, and include such suggestions as the right to delete and the right to be forgotten.[88] A recent European Court of Justice decision, holding that the right to be forgotten already exists in European law, has led to numerous requests by residents of the EU to have search engines remove personal information about them from search results.[89] This enthusiastic endorsement by the European public reinforces the acute need for legal and technological mitigation tools to address the proliferation of online information. It may well be that such tools evolve into more robust instruments that will eliminate information online completely upon request. On the other hand, strong opposing societal interests have led to calls to increase retention periods for data,[90] and of course, the recent revelations of government practices put the realization of such proposals into serious question.

6. FORMALIZING THE COLLECTION AND USE OF ONLINE INFORMATION

The *formalization* of the use of online information is yet another option, one which may be said to lie on the same path as that which

---

88 The proposed right to delete would enable individuals to request that information about them, harmful to their privacy (i.e. in the EU context, private life) be deleted from the database in which it exists. The proposed right to be forgotten would revive the longstanding principle of data minimization, as it applies to information retention. See 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* (Berlin, Germany: Nomos Publishers, 2009) 285, online: <http://www.ssrn.com/abstract=1401357>. See also Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, (Princeton: Princeton University Press, 2009).

89 The right exists but is subject to important limits. It can be exercised with respect to search engines, but not, so far, with respect to the Internet and databases more generally. See EC, *Factsheet on the "Right to be Forgotten" Ruling*, [2014] OJ C 131/12. In only a few months, Google received more than 90,000 requests. See Ben Fox Rubin, "Google granting majority of 'right to be forgotten' requests," *CNET* (25 July 2014), online: <http://www.cnet.com/news/google-granting-majority-of-right-to-be-forgotten-requests/>.

90 Those interests include freedom of speech, national security, and criminal investigations. In fact, it could be argued that as the cost of retention decreases, retention periods will continue to increase.

leads to the prohibited grounds approach. The processing of online information by employers when filling a job vacancy is often done informally, outside of the formal applicant evaluation process. Such an informal practice disadvantages not only younger applicants, on whom a more substantive digital dossier may exist, but also applicants who would otherwise be protected from discrimination under human rights legislation. The collection and use of such information in university and private school application decisions is another informal practice that may increase the risk of harm to members of groups that we wish as a society to protect.

Formalizing such processes may eliminate the risk of decision-making that would be in violation of human rights legislation. It may also offer some protection against harm to other privacy interests in online information. There have been calls for the application of statutory standards of fairness and transparency in the conduct of social media background checks and the evaluation of off-duty conduct.[91] In addition, non-binding guidelines have been put forward by privacy commissioners.[92] For example, employer requests for access to password-protected sites can be considered coercive in certain circumstances.[93] Formalization is in my opinion insufficient, since it is focused on the *process* of information collection (and use). In one sense, it stands in opposition to the proposed Oxford principles, since, rather than concede that the battle over collection has been lost, it imposes additional constraints on the collection of information. This stance may earn praise from privacy advocates, but in light of the enormous scale of collection by both government and the private sector, I question whether formalizing data collection is a viable approach.

If formalization of information collection is a lost cause, would formalizing the manner in which information is used offer applicants

---

91 See Carly Brandenburg, "The Newest Way to Screen Job Applicants: A Social Networker's Nightmare" (2008) 60:3 Federal Communications LJ 597; Ian Byrnside, "Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants" (2008) 10:2 Vand J Ent & Tech L 445.

92 See e.g. Office of the Information and Privacy Commissioner for British Columbia, "Guidelines for Social Media Background Checks" (Victoria: OIPC, 1 October 2011).

93 See *Pietrylo*, *supra* note 75.

greater privacy protection? In this sense, formalization is aligned with the Oxford principles, since both seek to control and constrain the use of personal information. However, where the Oxford principles offer a substantive harm/benefit evaluation as a form of (perhaps imperfect) constraint, the option of formalization focuses on internal organizational procedures. Formalization is a form of procedural constraint, and it may lead to more rigorous, transparent and accountable use — all very important and laudable goals. What formalization does not offer, though, is a substantive measure for the use of personal information. In the context of workplace privacy, it will not lead to the restriction of substantive action on the basis of personal information, if that information is not obviously (and perhaps clearly legally) part of a prohibited category.

Formalization does little, in other words, to minimize the broader harm caused by decisions based on non-discriminatory personal information that was obtained through breach of network privacy. To minimize the harm caused by breaches of network privacy, and to determine the proper measure in which online information should be used, it is necessary to focus on measures that restrict *actions* on the basis of online information and not only on rules that govern its processing. Substantive protection requires that constraints be set on the purposes for which such information can be processed. This is the goal which the Oxford principles aim to achieve through their suggestion of a harm/benefit analysis for personal information use. As noted above, it is far from clear whether the Oxford approach advances the privacy of employees and applicants, as a few concrete examples will illustrate.

7. THE PROHIBITED GROUNDS APPROACH

It is in the offer of a mixture of substantive and procedural measures that the significance of the prohibited ground model lies. Prohibited grounds information is information that is known (i.e., collected, whether deliberately or inadvertently) and available to act upon — but it is the *action* upon it which is forbidden.

If we accept the proposition that information online will be available to employers, educational institutions and other members of society, and that organizations will only increase their collection of such information, we must look for a proposal that will limit the

actions of those organizations on the basis of online information. Such a proposal should be aimed at limiting harm to the network privacy of individuals. What individuals find most troubling about the use of online information is the loss of real-world control, and the resulting blurring of boundaries between work and personal life. As a result, contexts disappear, and information that we carefully aim to keep separate for respective social circles (such as our employer, our family, our high-school friends) leaks across boundaries in a permanent, accessible and widely-spread fashion.

I propose therefore to limit action that can be taken against individuals on the basis of online information. Individuals would be protected from such action where the information obtained online does not harm other members of society. On the other hand, my proposal contemplates that criminal, unethical or truly harmful activities will not be protected, even in situations where these are evidenced exclusively online.

I suggest that these limits take the form of the prohibited grounds framework. The rules of the prohibited grounds framework are simple. If a piece of information falls within one of the categories that are prohibited, then no action can be taken on the basis of that information. Obviously, such rules cannot be directly applied to all online information. Put differently, the mere fact that information is *online* does not render it prohibited. We can imagine many cases in which we will want to allow, perhaps even require, employers to take action against current or prospective employees on the basis of online information. However, in order to protect network privacy, we should seek to restrict as much as possible action taken *exclusively* on the basis of information online, and to require supportive information from other, real-world, sources. In this way, we would endeavour to prohibit action based on online information when that information reveals aspects of an individual's private life but does not harm other members of society or violate criminal law or legally required ethical norms.

The proposal can be summed up in three substantive and procedural principles:

(1) *Individuals are protected from action against them on the basis of their online information, unless the information reveals criminal or illegal or unethical conduct or has caused significant harm.*

and,

> (2) *Individuals have a right to rebut online information if it is to be used against them.*[94]

and, in all other cases (i.e., when the concern is not about potentially criminal, illegal, unethical or significantly harmful behaviour),

> (3) *Online information must be supported by offline information if it is to be used against individuals.*[95]

Online information would thus be akin to a prohibited ground. Action on its basis, by and large, would be prohibited, or would require additional, supportive information from other sources which demonstrate that the action is based on other substantive grounds. To illustrate how such a limitation would work in practice, let us consider several workplace examples.

In cases that made headlines, employers have disciplined employees on the basis of online information from sources such as blogs, video clips and social network posts. For instance, a waitress lost her job after calling a customer "cheap" in an online Facebook rant.[96] A banking intern lost his job after being caught in a lie. Having told his managers that "something had come up at home," he showed up on Facebook in a fairy outfit at a costume party.[97] Two Domino's Pizza employees were fired after posting a video clip on YouTube that showed them preparing sandwiches at work while one put cheese

---

94 Even if the allegation is that they engaged in criminal, unethical or very harmful conduct.

95 These distil the discussion in Abril, Levin & Del Riego, *supra* note 13 at 121-123.

96 Frazier, *supra* note 20.

97 Helen A S Popkin, "Evolution Demands More Facebook Drunkfail," *MSNBC* (30 December 2008), online: <http://www.msnbc.msn.com/id/28424059/ns/technology_and_science-tech_and_gadgets/>; Owen Thomas, "Bank Intern Busted by Facebook" (12 November 2007), *Gawker* (blog), online: <http://www.gawker.com/321802/bank-intern-busted-by-facebook>.

up his nose.[98] The employees who were disciplined or dismissed in these examples indicated that they felt their privacy had been invaded.

First, let us take a look at the pizza waitress who was dismissed exclusively on the basis of her Facebook rant.[99] Under the rules of the proposal above, her employer would first have to demonstrate that this rant amounts to criminal or unethical behaviour or that it caused significant harm. While the rant is certainly not criminal, it may be unethical, and it may, depending on how widely it circulated and whether it identified the customer, cause significant harm. These are both questions of substance. Even if we assume that the employer can succeed in demonstrating one or the other, the employee would have the right to rebut the information. Apart from demonstrating that significant harm occurred, or a breach of an ethical obligation, the employer would have to adduce other, real-world evidence about the employee's poor performance in support of her dismissal. Again, even if we assume that the rant is a clear-cut example of an ethical breach or cause of harm, several factors would work against the employer in this scenario: the waitress had a strong expectation of network privacy, as her post was available only to her Facebook friends (one of whom apparently forwarded it to her employer); her at-work performance was not otherwise at issue; and her employer was not financially harmed. I would conclude that under the prohibited grounds model, the waitress's dismissal would not have been upheld, and her right to a private life online would have been protected.

How does the waitress fare under the Oxford proposal? Under the Oxford principles, there would have to be a determination of whether the employee was harmed (as defined by the principles) or whether the use of the online rant to dismiss her was simply an appropriate use and therefore permissible, regardless of its negative impact. If we assume that the use of online information is not always permissible, and was indeed harmful in this case, the employer would have to demonstrate that the benefit of dismissing the waitress outweighed the harm caused by her dismissal. Since this analysis can include the benefit to the employer and to society, it is not at all clear that it would

98 Stephanie Clifford, "Video Prank at Domino's Taints Brand," *The New York Times* (16 April 2009) B1, online: <http://www.nytimes.com>.

99 Frazier, *supra* note 20.

result in the dismissal being set aside, especially if the employer could demonstrate the existence of some policy or code of conduct covering off-duty behaviour. In contrast to the prohibited grounds framework, there is no default prohibition on the use of personal information, and the waitress in this case faces a greater procedural burden.

Now let us look at the partying intern.[100] Under the prohibited grounds framework, the employer would have to demonstrate that the intern committed a crime, behaved unethically, or caused significant harm, before it could use the online information. It seems reasonable to assume that the act of lying to his managers about his health would constitute unethical behaviour, and therefore meet this criterion. The employee would be permitted to rebut the presumed conclusion that he lied about his health, which would appear difficult given the large numbers of party-goers who had observed him. Finally, even if we deny that the conduct in question is unethical, the employer would be able to support action against the intern by providing real-world evidence about the true state of his health, which could be done by questioning his friends and fellow revellers. Although procedurally more cumbersome, the employer would still be able to achieve its desired disciplinary goal. It is important to note in this example that although the banker-to-be may have had strong expectations of network-privacy, since his photo was posted on Facebook exclusively for his friends (one of whom then kindly forwarded it to management), this expectation did not trump the legitimate employer interests. Network privacy is not an absolute right, and it can be defeated by other rights and interests, depending on the circumstances, as it would be here, once the intern presumably failed in his rebuttal.

Unsurprisingly, the banker does not fare well under the Oxford proposal. The employer here can make a stronger case that the use of the Facebook post is "appropriate" and does not meet the definition of harm. In this example as well, if we were to proceed to a harm/benefit analysis, it would be easier for the employer to argue that the benefits to society and to it outweigh the harm caused by the dismissal of a dishonest banking intern. The Oxford framework does not provide the intern with any greater procedural or substantive protection of his online privacy than the prohibited grounds framework.

---

100 Popkin, *supra* note 97.

Finally, let us look at the Domino's Pizza employees who compromised the health of their customers and immortalized their actions on YouTube.[101] In this example, too, the employees would not enjoy privacy protection by default with respect to their online information. Most observers would reasonably conclude that such conduct is unethical and in violation of the applicable health and safety legislation and regulations. Under the prohibited grounds framework, the employees would still be given an opportunity to rebut the evidence presented in the YouTube video. However, they would then most likely be disciplined. Under the Oxford framework, there would be yet a stronger argument that use of the online video against the employees is appropriate, and a yet stronger case that the benefits of discipline outweigh the harm suffered by the employees (if it is concluded that this use does meet the Oxford definition of harm).

Several points are illustrated by these examples. First, the Oxford principles do not offer, when applied to online information, any great substantive, or for that matter procedural, protection of employee privacy. Second, the Oxford principles are intended to guide a data protection regime, and do not capture the nuances of network privacy and its distinct meaning of harm. Third, the prohibited grounds framework does not radically transform or undermine the common law rules of evidence and its admissibility, thanks to the exceptions it makes for criminal, illegal and unethical conduct, and actions that cause significant harm.[102] Finally, the outcomes reached by the application of the prohibited grounds model to the examples will hopefully seem intuitively right to the reader. The model strikes an appropriate balance between *not* protecting individuals who have been involved in nefarious affairs, and preventing harm to individuals *exclusively* because online media have made their information accessible across contexts and boundaries. It maintains a clear-headed

---

101 Clifford, *supra* note 98 at B1.

102 That is not to agree that expectations of privacy in potential evidence, as governed by section 8 of the *Charter* (or by the Fourth Amendment to the United States Constitution) are correct. Indeed, it could be argued, and it has been argued, albeit unsuccessfully, that the law should recognize privacy expectations in real-world evidence such as sealed envelopes and garbage put to the curb. See e.g. *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579. I am grateful to Professor Adell for this point.

recognition that sometimes online information is indeed the tip of an offline "iceberg."

8. CONCLUSION

A decreasing number of employees in Canada and other countries enjoy the protection that a union and arbitral jurisprudence can afford to their privacy interests in online personal information. Even this minority among employees continues to be governed by principles established decades ago.[103] The large majority of non-unionized employees in Canada and other jurisdictions enjoy little or no procedural or substantive protection in their personal information online.

At the same time, the increasing permanency and availability of personal information that modern technology facilitates, and that private-sector and government activities exploit, is changing our social norms about information. Personal information protection legislation, in Canada and elsewhere, was designed for an era of relatively small databases, computer mainframes, and information that had a life-cycle with clearly defined stages of collection, use and disclosure. We are losing the battle against unfettered information collection, and the fear is that ultimately we will lose whatever legal protection that personal information currently enjoys.

Personal information is increasingly used and disclosed for purposes for which it was not collected or contributed. Those purposes include serving as evidence in litigation, as a basis for hiring decisions, and as justification for workplace disciplinary proceedings, educational application decisions, and generally at the critical junctures of modern-day life. Ironically, the wholesale collection and analysis of personal information may very well culminate in the circumvention of human rights and the prohibited grounds model.[104] For the generations of children and young adults growing up with a

---

103 The *Millhaven* decision regarding off-duty conduct dates from 1967. See *Millhaven Fibres Ltd v Oil, Chemical & Atomic, Workers Int'l Union, Local 9-670* (1967), 1A UMAC 328 (Anderson). But see the more recent decisions discussed above, which attempt to apply the *Millhaven* approach to the online world.

104 Solon Barocas & Andrew D Selbst, "Big Data's Disparate Impact" (2014) [unpublished, archived at SSRN], online: <http://www.ssrn.com/abstract=2477899>.

digital dossier that will accompany them throughout their lives, this is a matter of great importance, and yet a subject of little awareness.

This paper's proposal, to frame online information as if it were a prohibited ground of action, may seem far-reaching to some and its details require further refinement. If endorsed and adopted, it would ultimately lead to a substantive change of the regulatory framework protecting personal information in Canada within the employment relationship and throughout society more generally. Online information would be protected even if it does not fit the traditional definition of "personal information" that deserves privacy, and actions on the basis of online information would not be allowed unless additional criteria were met. Our privacy has been suffering defeat at the hands of government and corporations in an increasingly digitized, connected and surveilled world. We are in dire need of new defences, so that we can ultimately win this war in favour of our privacy, liberty and human rights.