The Future of Privacy:

Personal Information Protection Online

by Avner Levin*

Background

This paper has inevitably been shaped by the revelations of government electronic surveillance and (to a lesser extent) corporate surveillance and breaches of privacy conducted by the United States and several of its allies.[1] The revelations about the magnitude of the American National Security Agency's (NSA) surveillance programs dwarf the more mundane privacy concerns typically raised in commercial or other contexts. Ironically, around the same time news broke about the NSA, the Organization for Economic Co-operation and Development (OECD) was finishing the touches on the first revision to the OECD 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 the guidelines incorporated were: mandatory data breach notification, organizational privacy management programs, and national privacy strategies (again, the irony cannot go

* Associate Professor and Director, Privacy Institute, Ryerson University. This paper is an excerpt of a forthcoming paper in the Canadian Labour and Employment Law Journal

[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 http://www.theguardian.com/world/the-nsa-files [last accessed January 17 2014]

[2] For information on the OECD process see http://www.oecd.org/sti/ieconomy/privacy.htm [last accessed January 17 2014]

[3] The guidelines were created through the work of the OECD's privacy expert group. See OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", OECD Digital Economy Papers, No. 229, OECD Publishing. http://dx.doi.org/10.1787/5k3xz5zmj2mx-en [last accessed January 17 2014]

unnoticed).[4] However, the timing of their adoption presented an opportunity for some to call for more radical revisions.

The Oxford Internet Institute organized a workshop early in 2013 that produced a white paper titled *Data Protection Principles for the 21st Century*.[5] The proposed principles were meant to address the privacy concerns around "big data" and were not based on the NSA revelations.[6] Despite that, 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, and strengthens the principles that govern and restrict data use.[8]

The Oxford principles have been the subject of some controversy and perhaps mis-interpretation since their release late in 2013.[9] They are discussed in some detail in this paper, since this paper argues that one of the lessons already learnt from the NSA revelations is that 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

[4] For the revised guidelines in full see http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [last accessed January 17 2014]
[5] For the paper see http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf [last accessed January 17 2014]
[6] "Big data" is the popular term for the extremely large amounts of information collected for commercial purposes. Increasingly sophisticated analytical algorithms, yet to be developed, are supposed to unlock the insights that exist within these massive data sets.
[7] Supra note 5 at 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 are required depends on the jurisdiction and circumstances of collection.
[8] Supra note 5 at 8.
[9] For example, they were denounced by Ontario's Information and Privacy Commissioner. See https://www.privacyassociation.org/privacy_perspectives/post/so_glad_you_didnt_say_that_a_response_to_viktor_mayer_schoenberger [last accessed January 17 2014]

of Canada's personal information legislation,[10] as well as the OECD and other jurisdictions, and so such an argument is disheartening, to say the least. However, this paper continues to argue that the 'war' over privacy, if such a term can be used, will be fought and hopefully one over another fundamental principle – that of limiting the use of personal information.[11] Indeed, this paper argues that the principle of limited use should be strengthened and upgraded so that in some, although not all, circumstances the use of personal information obtained from online sources will be prohibited outright, just as the use of some personal information collected off-line – such as information about a person's race or gender is considered discriminatory.

The framework of "prohibited grounds" established by the Canadian Charter of Rights and Freedoms, and consequently, by federal and provincial human right codes should in fact serve as the basis for the protection of privacy interests that the public has in online information in general.

To establish the argument that online information should, in certain circumstances, be treated similarly to prohibited grounds information, this paper proceeds in the following parts. First, the paper discusses the notion of online privacy and why personal information available online deserves protection. Second, the paper briefly reviews the Canadian legal framework protecting employees and Canadians generally from discrimination – the "prohibited grounds" framework. Third, the paper discusses the revised data protection principles proposed by the Oxford workshop and their applicability and practicality. Finally, the paper suggests the manner in which the "prohibited grounds" model could apply to online information, the circumstances in which online information should be treated as if it were "prohibited grounds" information, and

[10] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (hereinafter, PIPEDA), Schedule 1, 4.4 ("Principle 4 – Limiting Collection") http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html [last accessed January 17 2014]

[11] PIPEDA, Schedule 1, 4.5 ("Principle 5 - Principle 5 —Limiting Use, Disclosure, and Retention") http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html [last accessed January 17 2014]

the utility of this treatment through a few examples. In the end, the paper offers a normative argument for the crucial, future development of the notion of privacy online.

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 common wisdom that information available online is 'public', fair game for employers, government, adversaries and friends. For example, in one of the early social media litigation cases in Ontario, the Court opined that "[T]he plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site."[12] In fact, research demonstrates that participants and users of social media have strong privacy expectations, expectations that so far the law is yet to acknowledge.[13]

With colleagues, I have referred elsewhere to these expectations of privacy online as a notion of 'network privacy'.[14] Network privacy protects the need of individuals to create their identity and their persona online. Without such protection we would not be able to engage in the forms of identity formation that we take for granted in the offline world, and that sociologists such as Goffman have argued are essential for societal interaction.[15] Importantly, identity formation requires a fair deal 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.'[16] In the real world it is fairly easy, although not always completely possible, thanks to long-held and well

[12] *Murphy v. Perger* [2007] O.J. No. 5511 (S.C.J) (QL), at para.20.
[13] See generally Levin, A. and Sánchez Abril, P. (2009), Two Notions of Privacy Online. *Vanderbilt Journal of Entertainment & Technology Law*, 11: 1001-1051. I discuss below some promising recent production decisions Stewart v. Kempster, 2012 ONSC 7236; Garacci v. Ross, 2013 ONSC 5627
[14] Supra note 13, Section IV.
[15] Erving Goffman, The Presentation of Self in Everyday Life (1959).
[16] Supra note 15, 49.

established social norms, to control the manner in which this information is shared, and to share different information with different audiences, leading ultimately to the creation of distinct personas, such as an individual's professional identity, religious identity, social identity and others.

Online, however, due to the permanency of digital records, and the ease of their dissemination, the separation of our information to support distinct identities becomes so much more difficult, more so due the social nature of this particular information – information that is not intended to be secluded or protected, but shared and used to construct 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 by which technology enables the infringement of copyright and other intellectual property rights.

Network privacy is the notion that harm, worthy of a remedy, occurs, when information is shared indiscriminately across social network boundaries – for example when compromising information is transferred by so-called friends of an employee to an employer.[17] According to network privacy information shared with a specific social circle is intended, by the individual that provided it, to remain within that social circle. That individual places implicit confidence and trust in other members of the social circle, and the information is not intended to be shared outside the boundaries of that social circle without the control and permission of the individual that the information identifies. An employee, for example, may wish to complain about her

[17] See Strahilevitz,L., A Social Networks Theory of Privacy, 72 U. CHI. L. REV. 919 (2005).See generally Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2009).

manager, or her customers, to her friends, but will not want the manager or the customers to have access to her posts or tweets.[18]

It is important to note that the employee, and individuals more general, will not wish information to be shared not only because of concerns over real-world 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 construct her workplace persona and identity to fit such values.

Legal recognition of network privacy would turn the sense of harm experienced by individuals when their information is shared across social boundaries online, without their consent, into a basis for legal action, and would entail individuals to some 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 norms, social norms, practices of 'netiquette', are created to support network privacy.[19] 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 they exist, such tools focus on the handling of personal information by the social media operator, and its affiliates, but not on the sharing of information between the individuals that socialize online. That is unfortunate,

[18] I discuss below one such unfortunate example. Infra note 74
[19] Burkell, J., Fortier, A., Wong, L., and Simpson, J., "The View From Here: User-Centered Perspectives on Social Network Privacy" (2013). FIMS Library and Information Science Publications, Paper 25. http://ir.lib.uwo.ca/fimspub/25 [last accessed January 17 2014]

since social media corporations are best positioned to develop effective tools and policies to protect network privacy.[20] In their absence, one example of developing online social norms involves photo-tagging among teens, where the current norm is that identifying photos should be removed at the request of the individuals that appear in them.[21] The protection network privacy provides, if respected, is the protection of the sense of self and identity, of reputation and dignity, and it is entwined with the formation of all of these notions, especially, but not exclusively, with 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 and information sharing every time, over the supposed alternative of withdrawal from participation in social media.[22]

Understood in such a manner, as 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, and, importantly, 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 that have access to information. Because online privacy focuses on the control of information as it is shared across social networks it is concerned not about the question "how many people know" but about "*who* knows." Common arguments to dismiss privacy expectations, referencing such numbers of "Twitter Followers" or "Facebook Friends" to indicate that no privacy expectation exists, are irrelevant to network privacy. A sense of privacy online can co-exist with hundreds of friends having access to Facebook information, and instantly disappear when just one other individual – a parent – is informed. The online behaviour

[20] Supra note 13, 1047.
[21] Supra note 19, 14-15.
[22] Supra note 13, 1046.

of individuals is somewhat paradoxical, therefore – 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 – yet harmful action on the basis of this information is prohibited by law. Those circumstances exist with respect to information about individuals such as their sex, colour, age and other grounds – grounds that, by law, cannot be used against them – grounds that if used, would constitute discrimination – prohibited grounds. The next section provides a brief review of the prohibited grounds framework in Canada before turning to the application of this model to online information.

Prohibited Grounds

One publicly accepted model of limiting action on the basis of publicly available information is the prohibited grounds model. Members of Canadian society are prohibited from acting against individuals on the basis of prohibited grounds, which are listed in our federal and provincial human right codes.[23] These are substantive grounds upon which discrimination is prohibited – such as an individual's sex, colour or religion. Individuals have a right that decisions will not be made against them on the basis of a prohibited ground, although exceptions that allow for discriminatory treatment do exist within the legislation (for historical reasons as well the reflection of contemporary social mores).[24]

[23] See for example the *Canadian Human Rights Act* (R.S., 1985, c. H-6) sec. 3. For ease of reference citations below are limited to the Ontario Human Rights Code (R.S.O. 1990, c. H.19) (hereinafter OHRC) The differences across Canada between the legal protection of human rights do not impact the argument of this paper.

[24] 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 that specific group of people that share the same prohibited ground. OHRC, sec. 24.

The right to equal treatment extends to social interactions such as the workplace, contractual transactions, the receipt of goods and services, the use of facilities, housing decisions and memberships in associations and unions.[25] There are many forms in which discrimination and harassment can take place, such as discrimination because of association with a person, systemic discrimination, poisoned work environments, failure to act inclusively, and more.[26] Regardless of form, examined from the perspective of personal information protection principles, discrimination and harassment are properly understood as forbidden purposes of information use. Of course, the act of collecting personal information can be itself discriminatory or lead to a strong 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.[27]

Indeed, published guidelines include detailed instructions regarding the permissible collection on application forms, as well as the permissible collection during interviews.[28] By and large explicit information collection is prohibited. Yet note that collection of personal information on many of the prohibited grounds is inadvertent and unavoidable. Take the full list of prohibited grounds with respect to employment in the province of Ontario as an example: 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.[29] 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 are then inferred as the interaction continues, such as ancestry, place of origin and ethnic origin from a

[25] OHRC, Part I.
[26] Supra note **Error! Bookmark not defined.**, Ch. III, sec. 2
[27] OHRC, sec. 23
[28] Supra note **Error! Bookmark not defined.**, Ch. IV, sec. 4-5.
[29] OHRC, sec. 5.

person's dialect, accent and personal conduct. Still others are easily assumed, such as creed, sexual orientation, gender identity and gender expression, from a person's cloths and external appearance. In short, it is possible to inadvertently "collect" almost all of the personal information that is prohibited by human rights legislation.

While collection of personal information related to prohibited grounds is not condoned and actively discouraged, the principles at the basis of the prohibited grounds model focus on the prohibition of discriminatory use, recognizing as a practical matter that personal information may well be "collected" despite the best intentions of the collector. Employers are instructed therefore, that they are 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 adopted for the purposes of online information, then it is worthwhile inquiring into the exceptions – the situations that allow for action, or for the use of prohibited information. The principles that guide these exceptions may serve as building blocks to guide situations when the use of information collected online would be permissible as well. One well-known exception is that employment requirements must be "bona fide", i.e., rationally connected to the job, adopted in good faith, and reasonably necessary.[30] I discuss below how the same essential principles, of a rational connection between information and proposed use, good faith conduct, and reasonable necessity (the last also known as the requirement to accommodate to the point of undue hardship) – the balancing of interests, play a role in formulating the rules for use of personal information that originated online.

[30] This is a summary of the well-known Meiorin test. British Columbia (Public Service Employee Relations Commission) v. BCGSEU, [1999] 3 S.C.R. 3.

The Oxford Principles

As mentioned a few paragraphs above, the Oxford principles are an attempt to formulate "Data Protection Principles for the 21st Century."[31] The proposal for revised OECD guidelines was meant to address the changes that occurred in data processing since the late 1970s and early 1980s to the present day, with the challenges of "big data" analytics.[32] The proposal points out many of the commonly accepted flaws in the way that current data protection regimes work, such as the privacy policies that individuals do not bother to read, or the terms of use that individuals "agree" to with the click of a mouse button.[33] These were meant originally to provide individuals with notice about the ways in which their personal information is 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 of the last decade has been the erosion of control, with privacy policies and "click-wrap" agreements serving to whitewash questionable information practices.[34]

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.[35] The culmination of several of workshops in 2012 and 2013, the proposal represents the joint work of academics, former data protection regulators and industry professionals, and was released late in 2013. The stated goal of the group, as mentioned above, was to shift the responsibility for the protection of personal information off the shoulders of individuals and place it with the

[31] Supra note 5
[32] Supra note 5, p.5-6.
[33] Supra note 5, p.7.
[34] Supra note 5, p.7.
[35] Supra note 5, p.8.

organizations that process the information.[36] The proposal attempts to achieve that goal by moving from the discredited notice and consent based model to a model focussed on permissible use, hence the potential relevance for this paper.

At the heart of the proposal stand its new, revised data principles, and their accompanying revised definitions of concepts related to personal information.[37] It refers to all data-related activity as information processing.[38] Within processing, four categories are proposed – information collection, use, storage and destruction.[39] The proposal suggests that the existing category of disclosure (of information to third parties) become part of the broader category of use, a move that would facilitate both the movement of data and the accountability of organizations.[40] 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 of more personal information; and the disclosure or dissemination of personal information to others.[41]

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.[42] It is this revision, the elimination of the requirement of consent to collection, which has drawn the most attention

[36] Supra note 5, p.11.
[37] Supra note 5, p.12-21.
[38] Supra note 5, p.14.
[39] Supra note 5, p.14.
[40] Supra note 5, p.16.
[41] Supra note 5, p.14.
[42] Supra note 5, p.15.

of critics.[43] 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.[44] In light of Snowden's revelations it is worth noting that the collection principle does address government collection, prohibiting government collection not based on legal authority or for a legitimate purpose.[45]

The manner in which the war over privacy could perhaps yet be won is described by the proposal's *use principle*. Rather than listing 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.[46] The proposal defines harm as encompassing both tangible and intangible harm (e.g. the feeling of an invasion of privacy) but excludes from the definition of harm any negative results of the "appropriate" application of personal information to an individual.[47] Once the balancing of benefits and harms has commenced, the proposal suggests that use involving no or minimal harm should be allowed, that use resulting in significant harm (e.g., personal injury) should be prohibited, and that the middle ground should be allowed as long as appropriate protection is in place.[48] 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

[43] Supra note 9.
[44] Supra note 5, p.16.
[45] Supra note 5, p.15. Of course, proponents of the NSA programs have argued for their legitimacy.
[46] Supra note 5, p.16-17. Benefits could be to the individual, to others or to society at large.
[47] Supra note 5, p.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 such as the extension of financial credit or insurance products on the basis of personal information. If that is the case it is an unfortunate concession to commercial interests.
[48] Supra note 5, p.16-17.

meaningful, real and informed.[49] It is questionable whether such consent can exist in some social contexts such as an employment relationship or of an application for employment.[50]

The proposal includes two other use-related principles, one to ensure the quality of personal information (the *quality principle*, largely unchanged from existing personal information protection principles) and another to allow for individual access to their 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.[51] However, this right of access is only provided when the personal information is used to impact an individual's education, employment, health or finances, or to impact and other legal rights an individual may have.[52] Generally, this principle of individual participation prevents individuals from challenging and accessing their personal information if it used for commercial purposes (such as the delivery of targeted ads).

Of the four principles that address information processing in general, two that are largely unchanged (the *openness principle* and the *security principle*) require organizations to be open about their information practices, and to secure personal information under their control.[53] The third principle, the *accountability principle*, which essentially requires organizational compliance, has been revised to include the consequences of non-compliance for organizations,

[49] Supra note 5, p.17.

[50] When the telecommunications company Telus introduced voice recognition identification for its employees it sought employee consent as required by PIPEDA. Employees were informed that refusal to consent may result in progressive discipline. In the resulting dispute the Federal Court ruled that, while threats of disciplinary measures normally vitiate consent, informing employees of potential consequences does not amount to such a threat. Further, the Court ruled that disciplining employees for refusing to provide consent would not be a breach of PIPEDA. The Court's decision and analysis illustrate the inherent difficulty of the application of the consent principle to the workplace. See *Wansink v. TELUS*, [2007] 4 FCR 368 paras. 17-31

[51] Supra note 5, p.18-19. Note that the principle does not guarantee that such challenges will be successful.

[52] Supra note 5, p.19.

[53] Supra note 5, p.20.

in the form of liability for reasonably foreseeable harm.[54] The inclusion of legal liability within the principle is another tool the proposal uses, in conjunction with the modified use and collection principles, to shift responsibility for data protection from individuals to organizations.[55] That is the tack taken with 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, ensuring they will be taken into consideration by organizations that collect personal information.[56]

Taken in its entirety, the Oxford Proposal suggests a new model for the processing of information. This new model clearly distinguishes between information that can identify – and negatively impact – an individual, and information that cannot. It focuses on the former, and excludes the latter from its scope. Further, the proposal suggests that information should be collected without notifying or requiring the consent of individuals, 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 unfettered processing on the pretext of individual agreement.[57] 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 or not. Only uses that result in significant harm should be outright prohibited, and the proposal suggests that most uses should result in little harm, or in harm that

[54] Supra note 5, p.20.
[55] Supra note 5, p.21.
[56] Supra note 5, p.21.
[57] Supra note 5, p.16.

could be mitigated by other means, and therefore that most uses would be allowed.[58] To provide some context, it does not appear that decisions about employment – even the termination of employment – would be considered by the proposal's standards to cause individual's significant harm, although the proposal does acknowledge that such uses of information do negatively impact individuals.[59] Further still, the proposal does allow individuals to engage organizations over their personal information in situations of information use that the proposal considers to negatively impact individuals, but it is understandable why the cumulative effect of these increasingly narrowing limitations led some critics to question the efficacy of the proposal overall to achieve its stated purpose of better organizational protection of personal information, and in the tentative conclusion that the Oxford Proposal unintentionally allows for the widespread processing of personal information with little restrictions. [60]

Online Information as a Prohibited Ground

If effective online privacy requires some concession to the reality of widespread personal information collection on the one hand, yet some substantive limitations on information use, and if the Oxford framework falls somewhat short in the provision of such limits, then what form should such limits take? I suggest in this section 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 its basis.

[58] Supra note 5, p.18.
[59] There is a subtle distinction here between harm and negative impact. The proposal does not consider the appropriate application of personal information harmful. Dismissal for cause, for example, would not be defined as 'harm'.
[60] See e.g., Cavoukian, A., Dix, A. & El Emam, K. The Unintended Consequences of Privacy Paternalism, *IPC Discussion Papers* (2014) [last accessed August 27 2014]

Obviously, such rules cannot be directly applied to online information – put differently, the 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, action on the basis of online information against individuals.

In what sense, therefore is the prohibited ground model applicable to online information? Up until recently, little or no thought was given to the origins of information in making a decision on its basis. In litigation, as mentioned above, with the promising exception of some recent procedural decisions that I discuss in the following paragraph, 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 was treated as public, with the number of friends often cited in support, and courts failed to consider that privacy online is contextual and network-specific.[61] 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.[62] Such decisions fail to recognize the notion of network privacy discussed above, in both an empirical and normative sense.

It may be that courts are developing a more nuanced understanding of privacy and information online. Two recent Ontario production decisions (procedural decisions on whether, in civil litigation, one party must produce the information demanded by the other party as part of the discovery process) are worth discussing in some detail. In the first, the defendant in a civil lawsuit over a traffic accident requested that the plaintiff produce all the vacation photographs she took after the accident, as well as all of her "private" Facebook account content.[63] The

[61] See e.g. *Murphy v. Perger* [2007] ,O.J. No. 5511 (S.C.J) (QL) Although see the recent decisions *Stewart v. Kempster*, 114 O.R. (3d) 151; *Garacci v. Ross*, 2013 ONSC 5627

[62] See *Re West Coast Mazda*, [2010] B.C.L.R.B.D. No. 190

[63] *Stewart v. Kempster* 114 O.R. (3d) 151, para. 1

plaintiff argued that her Facebook account served as her digital photo album.[64] 139 Facebook Friends had access to these photos and other content that she considered private.[65] The court, based on this number of friends, could have easily ruled, based on earlier decisions, that the plaintiff had no reasonable expectation of privacy in the photos.[66] Significantly, however, the court rejected that argument. These paragraphs are worth quoting in full:

> 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.[67]

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 and rights in the judicial process. The court recognizes that the number of individuals that have access to information may not be as important as the attempt of an individual to determine *who* will have access to their information.[68]

The court then considered the defendant's request to produce all 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

[64] Supra note 63, para. 4
[65] Supra note 63, para. 4
[66] That was the analysis in cases such as *Murphy v. Perger* supra note 61
[67] Supra note 63, paras.23-24 (emphasis added).
[68] Admittedly, the courts still have a way to go. A more critical read 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, the court in Stewart found reason to argue that 139 was a low number, by comparing it to 1 billion. Still, the contemplation that a person may have a privacy interest in information that is available to over one hundred people is noteworthy.

> 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**… 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.[69]

The court's recognition of a privacy interest in online information, and the analogy drawn by the court to written correspondence are interesting, given that privacy interests in real-world items such as filing cabinets and garbage cans have arguably been eroded as well.[70] Be that as it may, this decision may present growing recognition that there is privacy in online information, and that it does deserve legal protection. Indeed, a second recent decision appears to understand online privacy in this manner as well.[71] While the court did not engage in explicit privacy analysis, it did endorse the earlier understanding of the 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).[72] The parties were litigating over a traffic accident, the defendant again requested access to all of the photographs on the private section of the Facebook account, and the court characterized this request as a "high-tech fishing expedition" which should be denied.[73]

Hopefully such decisions will lead to greater recognition and acceptance of the notion of privacy online, in the courts and in arbitral decisions, not least because circumstances in which individuals are harmed in real life by their online activities have generated great media and

[69] Supra note 63, paras. 29,31.
[70] See also *infra* note 92
[71] *Garacci v Ross*, supra note 61
[72] Supra note 71, para. 9.
[73] Supra note 71, para. 9.

public interest. In some examples that made the headlines employers 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" on an online Facebook rant.[74] A banking intern lost his job after being caught in lie – he had told his bosses that "something had come up at home" and showed up on Facebook in a fairy outfit at a costume party.[75] 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 up his nose.[76] And collection is indeed increasingly unfettered. Employers are looking up information on applicants via search engines, data brokers, friends of friends, and requiring applicants to hand over passwords and access to their social networking profiles.[77]

Notwithstanding the Oxford proposal's definition of harm, the employees that were disciplined or terminated in these examples described, in addition to the harm they suffered due to the loss of their employment, their privacy as being invaded. There is currently no legislative or normative protection against that sense of invasion of privacy, which is, to use the terminology above, *network* privacy. The current Canadian regulatory regime does not view network-privacy as a form of personal information protection governed by existing legislation.[78]

---

[74] Eric Frazier, *Facebook Post Costs Waitress Her Job*, Charlotte Observer (May 17, 2010), http://www.charlotteobserver.com/2010/05/17/1440447/facebook-post-costs-waitress-her.html#ixzz19wkffGDz. [last accessed March 28 2014]

[75] Helen A.S. Popkin, *Evolution Demands More Facebook Drunkfail*, MSNBC (Dec. 30, 2008), http://www.msnbc.msn.com/id/28424059/ns/technology_and_science-tech_and_gadgets/ [last accessed March 28 2014]; Owen Thomas, *Bank Intern Busted by Facebook*, Gawker (Nov. 12, 2007), http://gawker.com/#!321802/bank-intern-busted-by-facebook. [last accessed March 28 2014]

[76] See Stephanie Clifford, *Video Prank at Domino's Taints Brand*, New York Times (Apr. 16, 2009) at B1.

[77] *Pietrylo v. Hillstone*, No. 06-5754-FSH, 2008 WL 6085437, (D.N.J. July 25, 2008); Neal Augenstein, Maryland *AG: Requiring Employees' Personal Passwords is Legal*, WTOP (February 23 2011) http://www.wtop.com/?nid=46&sid=2282721 [last accessed March 28 2014]

[78] Elizabeth Denham, *CIPPIC v. Facebook, PIPEDA* Case Summary #2009-008, http://priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm. [last accessed March 28 2014]

In addition to the Oxford principles, which I apply to these examples below in order to compare the Oxford approach to the Prohibited Grounds framework, there are of course other suggestions to tackle the increasing collection of personal information online. In the United States the relevant discussion has centred on personal health information (medical and genetic information), some of which exists online, and its attempted use by employers.[79] In Europe suggestions have been more general, emphasizing the notion of control over personal information. European-based attempts to mitigate the impact of online information include such suggestions as the right to delete and the right to be forgotten.[80] The recent European Court of Justice decision that the right to be forgotten already exists in European law,[81] has led to numerous requests by residents of the EU to search engines to remove personal information about them from search results.[82] This enthusiastic endorsement by the European public reinforces the great need for legal and technological mitigation tools for the proliferation of online information. It may well be that such tools evolve into more robust versions that would eliminate information online completely upon request, but there are strong opposing societal

[79] See .e.g., Heather Patterson, Contextual Expectations of Privacy in Self-Generated Health Information Flows, TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy (2013) Available at SSRN: http://ssrn.com/abstract=2242144 [last accessed August 27 2014]

[80] The proposed right to delete would be an individual right 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* Liability in the Third Millennium (ed. Aurelia Colombi Ciacchi et al., 2009), *available at* http://ssrn.com/abstract=1401357. See also Viktor Mayer-Schonberger, *Delete: The Virtue of Forgetting in the Digital Age* (2009).

[81] In an importantly limited form – the right exists with respect to search engines, but not, so far, with respect to the internet and databases more generally. See European Commission, Factsheet on the "Right to be Forgotten" Ruling, available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [last accessed August 27 2014]

[82] In only a few months Google received more than ninety thousand requests. See Ben Fox Rubin, Google Granting Majority of 'Right to be Forgotten' Requests, CNET (2014) available at http://www.cnet.com/news/google-granting-majority-of-right-to-be-forgotten-requests/ [last accessed August 27 2014]

interests that have led to calls to increase the retention periods of data,[83] and of course, the recent revelations of government practices that put the realization of such rights into serious question.

The *formalization* of the use of online information is yet another option, which may be considered to be along the path leading to the prohibited grounds approach. Unlike the formal discovery process, the processing of online information is often done informally. Such an informal practice disadvantages not only younger individuals, but also individuals that would otherwise be protected from discrimination under human rights legislation. Similarly, the collection and use of such information in university and private school application decisions is also an informal practice, and may cause greater harm to members of groups that we wish as a society to protect.

Formalizing such processes may eliminate decisions that would be in violation of human rights legislation. There are already calls for the application of statutory standards of fairness and transparency for social media background checks and evaluation of off-duty conduct,[84] as well as non-binding guidelines put forward by various privacy commissioners.[85] Employer requests for access to password-protected sites can be considered coercive in certain circumstances, for example.[86] Formalization is noteworthy, but 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 proposal to the Oxford principles, since it imposes more constraints on the collection of information, rather

[83] Such as freedom of speech, national security and criminal investigation interests. In fact, it could be argued that as the cost of retention decreases retention periods will continue to increase.

[84] See Carly Brandenburg, The Newest Way to Screen Job Applicants: A Social Networker's Nightmare (2008), *Federal Communications Law Journal* 60: 597; Ian Byrnside, Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants (2008), *Vanderbilt Journal of Entertainment and Technology Law* 10: 445.

[85] See e.g. Office of the Information and Privacy Commissioner for British Columbia, *Guidelines for Social Media Background Checks* (2011) available at http://www.oipc.bc.ca/guidance-documents/1454 [last accessed March 28 2014]; .

[86] See Pietrylo *supra* note 77

than conceding that the battle over collection has been lost. This principled stance may earn formalization praise from privacy advocates, but I question, given the enormous scale of collection by both government and the private sector, whether formalizing data collection is a viable approach.

If formalization of information collection is a lost cause, perhaps formalizing the manner in which information is used would offer us 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 the internal organizational procedures. Formalization is a form of procedural constraint, and it leads to perhaps more rigorous, transparent and accountable use – all very important and laudable goals in of themselves – but what formalization does not offer is a substantive measure for the use of personal information. 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 decision-makers basing their decisions 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 find 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 by rules governing its processing. Substantive protection requires setting constraints 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 I discussed above, it is far from clear that the Oxford approach contributes to

the privacy of individuals online, and I demonstrate that further through the discussion of some specific examples below.

It is in the offer of a mixture of substantive and procedural measures that the significance of the prohibited ground model for this paper 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 are to accept as given the proposition that information online will be available to members of society, and that organizations will only increase their collection of such information, we must look for a proposal which will limit the actions of these members of society on the basis of online information. Such a proposal should be aimed at negating the negative impact of online information as *online* information on our notion of network privacy (a notion, recall, which is based in real-world social interaction). What individuals find most troubling about the use of online information is the loss of that real-world control, and the resulting blurring of boundaries between work, personal life, and other aspects, so that 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, causing us harm along the way.

I propose therefore to limit action on the basis of online information so that individuals will be protected in instances where the information obtained online does not harm other members of society, and merely reveals to them aspects of an individual's private life. On the other hand, my proposal is that criminal, unethical and truly harmful activities will not be protected, even in situations where these are evidenced exclusively online. The proposal can be enhanced by considering additional "procedural" rules as follows:

I. 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,

II. Individuals have a right to rebut online information if it is to be used against them.[87]

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

III. Online information must be supported by off-line information if it is to be used against individuals.[88]

In such a manner online information would in fact 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 that would demonstrate that the action is based on other substantive grounds. To illustrate how such a limitation would work let us take a look at the workplace examples above, and imagine that the proposed prohibition was in place.

Let us take a look first at the pizza waitress – this employee was dismissed exclusively on the basis of her Facebook rant.[89] 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 widespread it is and whether it identified the customer, cause significant harm. These are both questions of substance. Even if we assume that the employer has succeeded in demonstrating one or the other, the employee would have the right to rebut the information,

[87] Even if the allegation is that they engaged in criminal, unethical or very harmful conduct.
[88] These distill the discussion in Blurred Boundaries, *supra* note **Error! Bookmark not defined.**, p.121-123.
[89] *Supra* note 74.

and the employer would have to support the rant with other, real-world evidence about the employee's poor performance in support of her dismissal, or else the waitress would keep her job. Again, even if we assume that the rant is clear-cut, several factors would still work against the employer in this scenario: the waitress had a strong expectation of network-privacy as her post was only available to her Facebook friends (one of which apparently forwarded it to her employer); her at-work performance was not an issue; and her employer was not financially harmed. I would conclude that under the Prohibited Grounds model suggested in this paper this waitress would not have been dismissed – her dismissal would not have been permitted, 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 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, then 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 result in a prohibition of the dismissal, especially if the employer would be able to demonstrate the existence of some policy or code of conduct covering off-duty behaviour, which more and more employers increasingly have. Unlike 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.[90] Under the Prohibited Grounds framework the employer would have to demonstrate that the intern committed a crime, behaved unethically, or caused significant harm, to be able to 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 a difficult fete to achieve given the large numbers of party-goers that observed him. Finally, even if we deny that the conduct in question is unethical, the employer would still be able to support action against the intern by providing real-world evidence about his real health, which could be done by questioning his friends and fellow revelers. Although procedurally more cumbersome, the employer would still be able to achieve the 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 in this case. 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. The partying intern example is a good example in which action on the basis of online information would be permissible under the Prohibited Grounds framework.

Unsurprisingly, the banker does not fare well under the Oxford proposal. There is a stronger case that can be made here by the employer that the use of the Facebook post is "appropriate" and does not even meet the definition of harm. And 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 the bank outweigh the harm caused by the dismissal of a dishonest

[90] *Supra* note 75.

banking intern. The Oxford framework does not provide the intern with any greater procedural or substantive protection of his online privacy, in comparison with the Prohibited Grounds framework proposed in this paper.

Finally, let us look at the Domino's Pizza employees who compromised the health of their customers and immortalized their actions on YouTube.[91] In this example as well the employees would not enjoy protection of privacy by default in their online information, as most observers would reasonably conclude that such conduct is unethical and in violation of the applicable health and safety legislation and regulations (although most likely not tantamount to criminal conduct). Under the Prohibited Grounds framework the employees would still be given an opportunity to rebut the evidence presented in the YouTube video, and then most likely disciplined. Under the Oxford framework there would be yet a stronger argument that the use of the online information (the video) against the employees is appropriate, and a 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 in these examples. First, that the Oxford principles do not offer, when applied to online information, any great substantive, or procedural for that matter, protection of privacy. Second, that 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, that the Prohibited Grounds framework does not radically transform or undermine the common law rules of evidence and its admissibility, even they protect online privacy by default. That is thanks to the exceptions made in the framework for criminal, illegal and unethical

[91] *Supra* note 76.

conduct (as well as actions that cause significant harm).[92] Finally, the outcomes reached by the application of the Prohibited Grounds model to the example will hopefully seem intuitively right to the reader**,** and to strike the appropriate balance between an interest *not* to protect individuals that have been involved in nefarious affairs, between a clear-headed recognition that sometimes online information is indeed the tip of an off-line "iceberg", and between an interest to not want to harm individuals *exclusively* because online media have made their information accessible across contexts and boundaries.

Conclusion

The increasing permanency and availability of personal information that modern technology facilitates, and that private sector and government activities exploit, is causing our social norms about information to change. 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 at all. Purposes such as serving as evidence in litigation, or serving as a basis for hiring decisions, or as information in support of workplace disciplinary proceedings, educational application decisions, and generally the critical junctures of modern-day life. Ironically, the wholesale collection and analysis of personal information may very well

[92] That is not to agree that the expectations of privacy in potential evidence, as governed by Sec. 8 of the Charter (or by the 4th Amendment to the United States Constitution) are correct. Indeed, it could be argued, and it has been argued, albeit unsuccessfully to-date, 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] 1 S.C.R. 579. I am grateful to Professor Adell for this point.

culminate in the circumvention of human rights and the prohibited grounds model.[93] For the generations of children and young adults growing up with a digital dossier that will accompany them throughout *their* lives this is of great relevance, and yet 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 adopted and endorsed it would ultimately lead to a substantive change of the regulatory framework protecting personal information in Canada. 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 without additional steps. In light of the defeat our privacy has been suffering 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.

[93] Barocas, Solon and Selbst, Andrew, Big Data's Disparate Impact. Available at SSRN: http://ssrn.com/abstract=2477899 [last accessed August 27 2014]