

**I Know What You Did Last Night (and this morning too):  
Protecting Your Anonymity in a World of Identifying Technologies**

(Version 2 for the Center for Innovation Law and Policy)

By Milana Homs  
University of Ottawa, Faculty of Common Law  
Faculty Supervisor: Professor Ian Kerr

October 31, 2003

GEORGE: (*On telephone*) “Could I speak to the Chief Inspector or someone in authority?...Well, Constable, I’d like to make a complaint about a disturbance of the peace at—I’d prefer it to be an anonymous complaint. Well, do you accept pseudonymous complaints?.... Never mind, my name is Wittgenstein...”

– Tom Stoppard, *Jumpers*

## I. Introduction

*Given the importance of anonymity to free speech, electronic commerce, and privacy, it is only a small exaggeration to suggest that the debate about anonymity on the Internet is in effect a debate about the degree of political and economic freedom that will be fostered, or tolerated, in a modern society.*

M. Froomkin, "Flood Control on the Information Ocean", *infra* note 22 at 395.

Lately, concerns have been raised about the trend towards identification in society. New commercial technologies that can pinpoint your geographic location, monitor what you read and download on the Internet, or block your access to a website because you come from a certain jurisdiction, cause worry because they eliminate our ability to act anonymously. Although the concept of these technologies is not new, having previously been employed in law enforcement, their use is: Used in a commercial context, these tools are leading to a loss of anonymity in the pursuit of customer identification for marketing, enforcement and legal purposes. Now, instead of our anonymity only being compromised for legitimate law enforcement purposes, we are at the mercy of the casual commercial or social observer.

Critics argue that this trend towards identification is threatening "to sharply diminish anonymity,"<sup>1</sup> and create a society filled with 'dataveillance', where our personal data is used to monitor and investigate our actions and communications.<sup>2</sup> According to Roger Clark, this trend towards "demands for identification in all manner of circumstances" is "rapidly undermining anonymity" and adversely changing the political nature of our societies.<sup>3</sup>

---

<sup>1</sup> J. Weinburg, Hardware-based ID, rights management, and trusted systems, *Stanford Law Review*. 52(5) at 1254 ["Hardware-based ID"].

<sup>2</sup> R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (1999), online: <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html> (last modified: 16 September 1999) ["Introduction to Dataveillance"].

<sup>3</sup> R. Clarke, "Certainty of Identity: A Fundamental Misconception, and a Fundamental Threat to Security" (2001) 8:3 *Privacy Law and Policy Reporter* 63-65.

What will a society inundated by identification technologies be like? The following are three scenarios which highlight the critical issues we will face if the trend towards identifying technologies is left unabated:

- *Scenario 1: A computer science student is researching encryption technologies on the Internet. He gets more and more frustrated as all the best encryption research sites, based at institutions in the United States, are blocked from him. He keeps getting error message after error message informing him that as a national of his country, he is not allowed to access these websites. A little later he is visited by a local police unit, questioning why he is trying to access encryption research sites.*
- *Scenario 2: A teenage girl is confronted by her angry father. He wants her to stop looking at alternative political sites on the Internet, as it is affecting his ability to be promoted at work. His boss pulled him aside earlier to warn him that as per company policy, digital profiles are purchased for promotional candidates. His profile lists dozens of 'subversive' websites recently visited and controversial reading material that has been downloaded.*
- *Scenario 3: A man is walking out of cigar store when his cell phone rings. It's his unhappy wife who immediately berates him for having visited the cigar store. She lists off the other places that he's visited in the last hour, and questions him suspiciously about why he spent so long sitting at a café. To her bewildered husband, she explains that she knows where he has been as the geo-locator service on his phone lets her know his location. Before she hangs up she tells him that his health insurance company called; his premiums have been increased because they found out that he had ordered cigars from an online retailer twice in the last month.*

These three scenarios describe what a world full of commercial identity tracking technologies could be like. Notable is the mix of both public and private uses of these technologies, a situation, according to Marc Rotenberg, “that the legal system has [not] encountered much before.”<sup>4</sup>

This essay discusses the concept of anonymity and the likely implications of its loss as a result of pervasive and unchecked utilization of identification technologies. Using the above three scenarios as illustrative of the unique dangers identification technologies present to society, this essay argues that the consequences of their use, especially on the ability to be anonymous, should be at the forefront of policy makers’ debates. Pursuant to this thesis, Part II of this essay defines the concept of anonymity. It will be shown that anonymity provides the conceptual foundation for far-reaching and fundamental “freedoms” society holds dear. Part III turns to the description of various identification technologies and how they enable others to monitor and record our daily activities, both online and off. Part IV focuses on the consequences and some of the individual and societal implications of the loss of our anonymity as a result of unchecked use of identification technologies. In the last part, I examine three possible solutions – law, technology and accountability – that strive to minimize the impact of these technologies. I conclude that there are viable solutions that can appropriately balance the needs of both consumers and corporations.

## **II. Defining concepts: What is anonymity?**

What is anonymity? Why should we want to protect it? Defining anonymity is the first step in understanding its value: Most broadly, anonymity is a state where we can disengage our activity from our identities. Dictionaries generally define it as a state of being of unknown name

---

<sup>4</sup> D. Farmer & C. Mann, “Surveillance Nation Part I” *Technology Review* (April 2003) 34 at 40 [“Surveillance Nation Part I”].

through lack of identification, personality or individuality,<sup>5</sup> basing the definition on anonymity's origins as a protection for authors and their writings.

The definition of anonymity has now gained a wider meaning: Gavison characterized anonymity as the extent to which an individual is subject to attention, and as one of three notions (secrecy, anonymity and solitude) that make up privacy.<sup>6</sup> G.T. Marx defines anonymity as being made up of seven categories of ways to identify an individual (identity knowledge) - only a person who cannot be identified in any of these categories is truly anonymous. These categories include: locatability, pseudonyms, pattern knowledge, social categorization, and symbols of eligibility.<sup>7</sup> Pseudonymity, as the word suggests, involves an identifier which cannot be directly linked to the person it describes. An example would be a false name given in a chat room – the name corresponds to the user, but the name is not the actual name of the user. With pseudonymity, an additional piece of information is required for an identification to be made.

Marx defines locatability as answering the question of “where, not who”, meaning that no actual address or name need be obtained, rather only “the ability to locate and take action such as blocking, granting access, charging, penalizing rewarding or apprehending.”<sup>8</sup> Identification through pattern knowledge refers to knowledge gained by correlated data where the “actual identity or locatability” of the person may not be known.<sup>9</sup> Although a person may remain unnamed through pattern knowledge (for example, a recorded IP address that is not connected to a name), it is possible to identify users with a high degree of probability through various fragments of information that compound to produce only a small pool of candidates.<sup>10</sup> Marx

---

<sup>5</sup> The Oxford English Dictionary, 2<sup>nd</sup> ed., s.v. “anonymity”.

<sup>6</sup> Gavison, Ruth, “Privacy and the Limits of Law” (1980) 89 *Yale Law Journal* at 428.

<sup>7</sup> G.T. Marx, “What’s in a Name? Some Reflections on the Sociology of Anonymity” (1999) 15 (2) *The Information Society* at 101.

<sup>8</sup> *Ibid.*

<sup>9</sup> *Ibid.*

<sup>10</sup> H. Nissenbaum, “The Meaning of Anonymity in the Information Age” (1999) 15 (2) *The Information Society* 142.

characterizes identification through symbols of eligibility as a process whereby a person's knowledge (passwords) or objects (security badges) that places them into the category of either eligible or non-eligible.

Like Marx, Clarke also explains anonymity by using the concept of identity. Clarke puts anonymity on a spectrum with pseudonymity and identification. He describes pseudonymity as being an alternate state to anonymity, one where you cannot in a "normal course of events" be linked back to your identity.<sup>11</sup> Identity, according to him, is "a set of information about an entity that differentiates it from other, similar entities."<sup>12</sup> Clarke explains these terms best through the framework of a data transaction:

An **anonymous** record or transaction is one whose data **cannot be associated with a particular individual**, either from the data itself, or by combining the transaction with other data.... An **identified** record or transaction is one in which the data **can be readily related to a particular individual**. This may be because it carries a direct identifier of the person concerned, or because it contains data which, in combination with other available data, links the data to a particular person.... A **pseudonymous** record or transaction is one that cannot, **in the normal course of events**, be associated with a particular individual.<sup>13</sup>

Clarke's differentiation between anonymous, identified and pseudonymous transactions is based on how the transactions relate to authentication by an information system. For instance, where the authentication system cannot relate a transaction to the particular individual, then the individual remains anonymous. Where the information system can relate it to a particular person then it is identifiable and the individual enjoys no anonymity. Finally, where the information system can ascertain certain discrete elements of information, but would require additional information to ascertain the individual's true identity, then the person transacting is

---

<sup>11</sup> R Clarke, "Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice" (1999), online: <http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html> (last modified: 30 April 1999) ["Identified, Anonymous"].

<sup>12</sup> *Ibid.*

<sup>13</sup> *Ibid.*, [emphasis added].

pseudonymous. As the key objective of identification technologies is to authenticate users, Clarke's conceptual framework is helpful in establishing where a person will be situated on the spectrum of identifiability.

Notwithstanding the many differing definitions of anonymity, everyone agrees that there is value to it.<sup>14</sup> Nissenbaum believes that the value of anonymity lies "in the possibility of acting while remaining out of reach",<sup>15</sup> and being able to participate in a transaction without one's identity being revealed.<sup>16</sup> Froomkin gives Internet examples of this type of conduct, such as participating in a discussion forum without giving one's name, creating digital personas (in online gaming, in chat sessions) to explore one's creative side, or searching for stigmatic information on the web (on sexually transmitted diseases, hair loss, incest).<sup>17</sup> Clarke argues that we want to conduct ourselves anonymously for several reasons, "such as avoiding physical harm, enabling 'whistle-blowing', avoiding unwanted and unjustified public exposure, and keeping personal data out of the hands of intrusive marketers and governments."<sup>18</sup>

These objectives of anonymity are desirable; yet, one must keep in mind that there are countervailing issues which militate against the maintenance of anonymity. For instance, Clarke argues that the reasons for wanting to be anonymous are of "significant social value",<sup>19</sup> however he cautions that anonymity can also be used as a means to ends which are of "dubious social value". Clarke cites criminal purposes (avoiding detection for immoral or illegal activity), escaping responsibilities and spreading rumours (i.e. posting libellous statements on a bulletin

---

<sup>14</sup> See Marx, *supra* note 7, for a discussion of the pros and cons of anonymity.

<sup>15</sup> Nissenbaum, *supra* note 10 at 142.

<sup>16</sup> *Ibid.*, at 141.

<sup>17</sup> Froomkin, A.M., "Legal Issues in Anonymity and Pseudonymity" (1999) 15 (2) *The Information Society* at 115 ["Legal Issues"].

<sup>18</sup> "Identified, Anonymous", *supra* note 11.

<sup>19</sup> *Ibid.*

board) as examples of anonymity being used to shelter anti-social behaviour.<sup>20</sup> This concern about anonymity has been echoed by others, most decisively in *McIntyre*, where Justice Scalia (for the minority) wrote that anonymity “facilitates wrongs by eliminating accountability, which is ordinarily the very purpose of the anonymity”.<sup>21</sup> Froomkin believes that Scalia’s opinion in *McIntyre* represents “the strongest moral objection to the increase in anonymous interaction” because it resonates with a societal fear not to have the opportunity to redress false claims.<sup>22</sup> Others, like Richard Posner, argue that we should not have a right to conceal ourselves from others at all, as often “the motive for concealment is...to mislead those with whom [we] transact.”<sup>23</sup>

Traditionally, anonymity’s value lay in allowing writers freedom of expression by not having to link their identities to their oftentimes controversial writings. In the U.S. the anonymously written Federalist Papers started a tradition of politically-motivated anonymous writing.<sup>24</sup> Since then U.S courts have held that anonymity can be used for constructive purposes, entrenching the right to anonymous writing and speech in the U.S. constitution.<sup>25</sup> The constructive purposes of anonymity have been defined as the right to speak and publish, to post on the internet,<sup>26</sup> and the right to receive information and ideas anonymously. As Bender J. in *Tattered Covers* opines “[e]veryone must be permitted to discover and consider the full range of

---

<sup>20</sup> *Ibid.*

<sup>21</sup> *McIntyre v. Ohio Election Commission*, 514 U.S. 334 (1995).

<sup>22</sup> M.A. Froomkin, “Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases” (1996) 15 *U. Pitts. J. L. & Com* at Part I (a) [“Flood Control”].

<sup>23</sup> Richard A. Posner, “The Right of Privacy” (1978) 12 (3) *Georgia Law Review* at 399.

<sup>24</sup> *The Federalist*, commonly referred to as the *Federalist Papers*, is a series of 85 essays written by Alexander Hamilton, John Jay, and James Madison between October 1787 and May 1788. The essays were published anonymously, under the pen name "Publius," in various New York state newspapers of the time.

<sup>25</sup> *Talley v. State of California*, 362 U.S. 60 (1960); *Tattered Cover, Inc v. City of Thornton*, 44 P.3d 1044 (Colo.2002). In the U.S. this constitutional guarantee was challenged and upheld in *McIntyre* (*supra* note 21) where a woman appealed from a fine for distributing unsigned political leaflets.

<sup>26</sup> *Doe v. 2TheMart.com, Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

expression and ideas available in our ‘marketplace of ideas,’” otherwise there will be chilling effects on the public’s willingness to read about controversial subjects.<sup>27</sup>

Anonymity has not been as much of a legally contested issue in Canada as it has been in the U.S.; very few Canadian cases make pronouncements about anonymity.<sup>28</sup> Most relevant is a 2002 Ontario case that dealt with a claim to disclose an Internet user’s identity, the court pronounced that a degree of confidentiality with respect to the identity of an Internet user “has significant safety value and is in keeping with what should be perceived as being good public policy.”<sup>29</sup> The court held that a user’s anonymity should not be given up lightly by an ISP, and that only where a prima facie case against an anonymous user has been established, is disclosure of the user’s identity appropriate.

Anonymity falls under the broader concept of control over the dissemination of personal information, otherwise known as informational privacy.<sup>30</sup> This concept is receiving much attention lately, as policy makers, companies and civil society struggle with the ethics of using our personal information in an information-based age. What is information privacy? According to Roger Clarke, “information privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.”<sup>31</sup> Informational privacy theorists argue that the personal data generated by our activities is private and worth protecting.

---

<sup>27</sup> *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002).

<sup>28</sup> This may be because Canadians rely on the “invisible fence” that the *Canadian Charter of Rights and Freedoms* “erect[s] around each individual” to protect their rights, including the right to anonymity (*R. v. Morgentaler*, [1988] 1 S.C.R. 30 at 164, Wilson J.). Other Canadian cases that rule on the concept of anonymity include *Phillip Services Corp. v. John Doe* (Ont Ct. Gen. Div. 1998), the first internet anonymity case, where the court granted a motion to have the identity released of several users alleged to have made fraudulent postings on a stock website. See also *R v. Plant* [1993] 3 S.C.R. 281. As well, Elections Canada has ordered a political party website removed because it allegedly “violated the Canada Elections Act by not disclosing the person responsible for the site”.(qtd. in Michael Geist, *Internet Law in Canada*, 3rd ed. (Toronto: Captus Press, 2002) at 381.

<sup>29</sup> *Irwin Toy Ltd. v. Doe*, [2000] O.J. No. 3318 at para 11.

<sup>30</sup> See generally J. Cohen, “A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace (1996) 28 *Conn. L. Rev* 981 [“A Right to Read Anonymously”]; Jessica Litman, “Information Privacy, Information Property,” (2000) 52 *Stanford Law Review* 1283.

<sup>31</sup> “Introduction to Dataveillance”, *supra* note 2.

They warn that a loss of informational privacy can lead to mass aggregation of our financial, medical, personal interest and activity data which would paint a complete picture of us.<sup>32</sup> Basically, where our personal information and transactions are aggregated they become more valuable than the sum of their parts by becoming an intimate and comprehensive picture of us, while when our information is fragmented it has less value. Clarke calls this complete picture our “digital persona”: a model of us “based on data, and maintained by transactions, and used as a proxy for the individual.”<sup>33</sup>

Where does anonymity fit into informational privacy, or rather, how do these two concepts relate? Marx and Fromkin argue that anonymity allows us to control information about our identity, thereby protecting our informational privacy.<sup>34</sup> According to Fromkin, “[a]nonymity may turn out to be the only tool available to ordinary people that can level the playing field against corporations and governments that might seek to use new data processing and data collection tools in ways that constrain the citizen’s transactional or political freedom.”<sup>35</sup> The distinction between anonymity and privacy is best explained with a practical example from our third scenario: A man buys a cigar with cash from a vendor at a busy intersection. The vendor knows that someone bought a cigar, but does not have a record of who the buyer was and cannot link the cash or the visit with an identity. The buyer remains anonymous. If the man buys the cigar from an online vendor instead, he instantly becomes non-anonymous as the online vendor at minimum keeps a record of the buyer’s mailing address and payment details. What the vendor does with the record relates to informational privacy: If he sells the data (e.g., what type of cigars that buyer bought, how many times that year he bought cigars) to a marketing firm,

---

<sup>32</sup> J. Cohen, “Examined Lives: Informational Privacy and the Subject as Object” (2000) 52 *Stan. L Rev.* at 1426 [“Examined Lives”].

<sup>33</sup> “Introduction to Dataveillance”, *supra* note 2.

<sup>34</sup> Marx, *supra* note 7 at 100.

<sup>35</sup> Fromkin, “Legal Issues”, *supra* note 17 at 115.

then he may be violating the buyer's informational privacy. The ultimate point is that anonymity lets us keep our digital persona incomplete by allowing us to enter into unrecorded transactions. Thus, in our example above, anonymity allows the buyer to shield himself from having his informational privacy compromised. The reasons why keeping our digital persona complete is important will be discussed in Section IV.

In this section I have defined anonymity as a state where we can disengage our activity from our identities or the 'digital persona' that has been created through our transactions. I have also described its value, as a tool for freedom of expression and action, which has been recognized in law as deserving of protection. In the next section, I examine the technologies which are currently threatening people's ability to remain anonymous.

### **III. The technologies that are affecting anonymity**

There are a myriad of identifying technologies that are affecting us; in this paper, I will concentrate on different forms of geo-location technology and digital rights management systems. I picked these technologies because they are new, they lack substantial regulation and their unchecked use has consequences for society and innovation. When reading about these technologies, the following two commonalities should be noted - they attempt to authenticate users and track their actions, and they are now available for commercial use.

#### **Geo-location technology**

Geotracking is the short form for "geographic location tracking". In the offline world, geotracking defines a wide range of Global Positioning System (GPS), cellular phone or other transmitting technology that allows a person or object to be located. A good example of this are the GPS devices installed on many rental cars that broadcast their position if they have been

stolen.<sup>36</sup> In the Internet context, geo-tracking is comprised of technology that allows a website to track and block its website visitors. Simplified, the technology usually uses algorithms to search constantly updated data sources to come up with an identity or location ('geo-location intelligence') behind a visitor's IP address.<sup>37</sup> It can selectively block users or deliver content based on geography, as well as gather valuable information about when and how often a user visits the location.

What sort of information can Internet geotracking gather? Although it cannot track the exact identity of a user, geotracking applications can identify geographic information such as a user's postal or zip code and business information such as the name of the visitor's company, organization or university.<sup>38</sup> This presents several issues for anonymity: Firstly, websites that use these applications restrict you from web surfing anonymously as your geographic location will be known. Recall that Marx identifies one of factors that make up anonymity as locatability, meaning if one is able to identify where you are located, then you are not truly anonymous. Knowing your approximate location may seem harmless to many, however for citizens in authoritarian states such as China and Saudi Arabia, such technology can be used to block their ability to surf the Internet with free will.<sup>39</sup> Similar to filtering technologies that do not (from the user's end) allow certain sites to be visited, geotracking technologies can block users (from the website's end) from certain locations. For example, as in the first scenario, such technology could be used to prevent users from certain countries from accessing a website on encryption technology in the United States.

---

<sup>36</sup> In Connecticut, a rental car company fined a renter for speeding. The time, place and exact speed of the incident had been monitored by the company, triggered by whenever the car crossed the speed limit, see Stenger, *infra* note 71.

<sup>37</sup> Verifia Inc., White Paper, "Internet Geography Guide" (2002) at 3.

<sup>38</sup> *Ibid.*

<sup>39</sup> J. Dettmer, "Regulators Ready to Put Chains on Cyberspace" (2001) 17:34 *Insight on News* at 13.

Even for users from democratic countries, ‘bordering the Internet’, as the use of geotracking is often coined, can also lead to less freedom in surfing the web. For instance, users from Canada cannot access Movielink, Sony’s movie download site, even for browsing purposes. Although Movielink blocks access for valid intellectual property licensing purposes, it foreshadows a World Wide Web where these technologies are widely used to regulate access. A worst case scenario is that the web will become ‘bordered’ so that access to websites becomes limited to citizens from ‘approved’ countries.

In the offline context, geo-location devices have recently shown up in rental cars and children’s locator wristbands.<sup>40</sup> Based on GPS technology, these devices can pinpoint your location to the nearest block. For example, the Wherify Geo Locator allows parents to locate their children within minutes, and comes with a safety lock to prevent removal of the wristband.<sup>41</sup> It also allows for ‘geo-fencing’ which lets parents to pre-set authorized areas for their children, and sets off an alert when children leave the area.<sup>42</sup> Similarly, many wireless carriers are developing geo-location services for cell phones, which will allow people, like in our third scenario, to pinpoint the exact location of a cell phone and track its recent history of locations.<sup>43</sup> These examples are just some of the new offline technologies that are emerging that seek to capitalize on the global reach of GPS technology and depend on society’s acquiescent move toward an identification and monitoring society.

---

<sup>40</sup> Stenger, *infra* note 71.

<sup>41</sup> Wherify GPS Locator for Children, online: [http://www.wherifywireless.com/prod\\_watches.htm](http://www.wherifywireless.com/prod_watches.htm) (date accessed: 1 May 2003).

<sup>42</sup> Rick Mathieson, “like ‘lojack’ for children: wireless location services in an age of endangered kids” *mpulse Magazine*, (November 2002), online: < <http://cooltown.hp.com/mpulse/1102-lojack.asp>> (date accessed: 1 May 2003).

<sup>43</sup> See Charny, *infra* note 69.

## P2P monitoring

A subset of internet geo-location technology is P2P monitoring services. These services are a type of geo-location technology that helps find copyright infringers on peer to peer (P2P) file sharing networks. P2P monitors use similar technology as geotracking to scrutinize P2P networks and correlate users IP addresses with available databases to find out the name of the user's organization or ISP. It has been used predominately by the music and movie industry to monitor popular P2P sites to discourage copyright infringement of their proprietary material. For example, in the summer of 2003 the Recording Industry Association of America (RIAA) began filing lawsuits against individual file sharers. The evidence against the file sharers is being gathered by using monitoring services in popular file sharing networks.<sup>44</sup> The Motion Picture Association of America (MPAA) has also begun using this technology and sent warnings to approximately 2000 people a week in 2002 about illegal movies being traded.<sup>45</sup>

The MPAA and RIAA subscribe to a geo-location service called Ranger Online which is geared specifically to violations of copyright infringement. Technology like Ranger that allows corporations to self-police is being aided in the U.S. by the *Digital Copyright Millennium Act*,<sup>46</sup> which compels ISPs to stop distribution of copyrighted materials when they are notified. The problem is that they do not have to be notified by a legitimate authority who ensures that there is a valid infringement, but rather by anyone who insists that their copyright is being infringed.

---

<sup>44</sup> RIAA, "Recording Industry To Begin Collecting Evidence And Preparing Lawsuits Against File "Sharers" Who Illegally Offer Music Online" *Press Release* (25 June 2003), online: <<http://www.riaa.com/news/newsletter/062503.asp>> (date accessed: 1 August 2003).

<sup>45</sup> B. Sullivan, "Hollywood gets tough on copying" *MSNBC* (12 July 2002), online: (date accessed 6 January 2003). <http://www.msnbc.com/news/779198.asp?cp1=1>. See also Janelle Brown, "Who is spying on your downloads?" *Salon Magazine* (27 March 2001), online: <[http://dir.salon.com/tech/feature/2001/03/27/media\\_tracker/index.html?pn=1](http://dir.salon.com/tech/feature/2001/03/27/media_tracker/index.html?pn=1)>; Declan McCullagh, "Perspective: The new jailbird jingle" *News. Com* (27 January 2001), online: <<http://news.com.com/2010-1071-982121.html>>; Frank Ahrens, "Ranger Vs. the Movie Pirates" *Washington Post* (19 June 2002) H01, online: <<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A5144-2002Jun18&notFound=true>>.

<sup>46</sup> Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

Thus, legislation is working in tandem with new technology in order to create a culture of self-policing, where companies take the lead in searching out violations against themselves using commercial services like Ranger, and exerting pressure on ISPs to reveal the identities of their users. Although the RIAA and MPAA have a right to be concerned with copyright infringement, that right comes into direct conflict with other peoples' corollary right to not have their every movement on the internet recorded and scrutinized. The average user must think twice -- their Internet downloading actions are not as anonymous and unidentifiable to outsiders as they may have thought.<sup>47</sup>

### **Copyright Management Systems**

Another type of identification technology that affects anonymity is copyright management systems (also known as 'trusted systems' or digital rights management systems), which make digital content available only to computer systems that have been identified.<sup>48</sup> This technology allows copyright owners: to prevent their work from being disseminated on peer to peer networks; to stop their work from reaching jurisdictions where it shouldn't be distributed; or simply to know who is using their systems. An innocuous example of a trusted system and its effects is online newspapers requiring registration, such as the New York Times Online Edition. If you read the news on the New York Times website for any significant length of time, the Times will have created an extensive profile on you based on what type of news you read and how often you read it; all linked to your email address and name.

While, on the one hand these systems offer copyright holders a way to protect their goods from piracy and infringement, on the other hand they have negative consequences on peoples' ability to remain anonymous. First, users must be authenticated before being able to use them,

---

<sup>47</sup> It should be noted that workplace system operators can and often do log all the websites visited by users of their networks.

<sup>48</sup> "Hardware-based ID", *supra* note 1 at 4.

meaning that you cannot be truly anonymous and use these systems.<sup>49</sup> At the authentication stage, users must usually provide basic information such as a credit card number, postal address and email information. There is usually no option of bargaining with a system in order to preserve your anonymity: If you do not authenticate yourself, you cannot access the system. Cohen summarizes the problem aptly: “A right to read anonymously cannot be preserved if it must first be bargained for on a case by case basis: the act of bargaining negates the goal of concealment.”<sup>50</sup>

The second implication to anonymity that the use of these types of systems present is that, once authenticated, these systems can monitor a user’s use of the materials on the system. This monitoring includes knowing every time someone accesses a piece and how they access it, thereby allowing a complete profile to be made of the user’s habits, likes and dislikes.<sup>51</sup> This is a veritable treasure trove for data profiling companies, according to Fromkin, who argues that that our reading habits will certainly be chilled if visits to websites “leave a data trail behind it.”<sup>52</sup> An extreme example of how are reading will be chilled is the second scenario in Part I, where the daughter is asked to stop reading controversial news material because her father is fearful he will not get promoted. A real life example of how this type of monitoring works occurred with Real Networks’ Realplayer music system.<sup>53</sup> The software installed a global unique identifier (GUID) on a user’s computer which transmitted to Real Networks information about the music stored on the host computer and what CDs were played. This information was linked to the user by the email address given at registration, allowing the company to have a complete picture of an email

---

<sup>49</sup>. You could preserve your anonymity by authenticating yourself with a fraudulent identity.

<sup>50</sup> “A Right to Read Anonymously”, *supra* note 30 at 981

<sup>51</sup> Weinburg *supra* note 1 at 1269. See also “A Right to Read Anonymously”, *supra* note 30 at 981.

<sup>52</sup> “Flood Control”, *supra* note 22.

<sup>53</sup> Weinburg, *supra* note 1 at 1261-1262.

address's music preferences. After much public pressure Real Networks eventually offered a software patch that would disable the GUID, however this may not be the result in future cases.

If GUIDs and their ilk become part of our daily reality, the ability to be anonymous in our personal lives will become more and more difficult, as our actions will increasingly be logged, rather than left unrecorded. In the next section I will detail what I believe are three important implications to this growth of identification technologies.

#### **IV. Implications of identity technologies**

There are three main implications for society of a loss of anonymity. The first is that the aggregation of data about each individual's internet activities will lead to almost perfect profiling of the individual. Second, the profiling will lead to mainstreaming of choices, as people avoid actions that will single them out in any way. Third, the ability to identify individuals will lead to widespread self-regulation by corporations of actions they perceive to be wrongs.

##### **A. Our digital persona**

As mentioned earlier, one of the implications to a loss of anonymity is the creation of what Roger Clarke calls our digital persona. A digital persona is an almost perfect model of who we are based on data collected about us through our transactions and activities, and linked to us through an email address, an IP address, or a name. It is not the recording of a singular transaction that is worrisome, but rather the practice of aggregating these non-anonymous transactions and linking the total picture back to the transactor. As Farmer and Mann have recently written "each type of monitoring may be beneficial in itself, at least for the people who put it in place, but the collective result could be calamitous."<sup>54</sup> Having a digital persona is worrisome because it allows strangers, employers, marketers and anyone else who cares to put

---

<sup>54</sup> Mann and Farmer, *supra* note 4 at 73.

the effort in to glean a complete picture of our current and past actions and intentions, whether good, dubious or bad.

The ability to link identifiable information with our activity and transaction data already exists. For example, Doubleclick, the Internet banner advertising company, was close to linking its database of Internet activity data to a marketing database of more than 2 billion personally identifiable consumer catalog transactions when it purchased Abacus Direct, a market research company. However, as was done in the Real Networks case, Doubleclick scuttled its plans to combine the two databases after intense public pressure.<sup>55</sup>

According to Fromkin, profiling from our non-anonymous use of trusted systems will only grow as our medical histories, grocery purchases, personal movements (through geo-location devices) and financial transactions join our reading and viewing habits to give marketers a complete picture of who we are.<sup>56</sup> Some argue that this may not be a negative implication: For example, Dave Amis has written that profiling may be beneficial in that it results in the more precise targeting of ads: “The prospect of actually being able to view ads that are relevant to our needs and interests is something to be positively welcomed”.<sup>57</sup>

Unfortunately, marketers’ using our profiles is not the most contentious use of profiling. For instance, Weinburg believes that profiling will lead to undesirable social consequences<sup>58</sup> when the use of profiling goes beyond marketing, and is used, like in our scenarios, by insurance companies, potential landlords or employers. Cohen gives examples of employment decisions and classifications based on health information gathered through profiling activities, and

---

<sup>55</sup> Evan Hansen, “DoubleClick postpones data-merging plan” *CNET News.com* (2 March 2000), online: <<<http://news.com.com/2100-1023-237532.html?legacy=cnet&dtm.head>> (date accessed: 10 March 2003).

<sup>56</sup> “Flood Control”, *supra* note 22.

<sup>57</sup> Dave Amis, “Online Profiling - a threat or a benefit?” *Internet Freedom News* (1 February 2000) <http://www.netfreedom.org/news.asp?item=106> (date accessed 30 March 03).

<sup>58</sup> “Hardware Based ID”, *supra* note 1 at 1269.

employment or housing decisions based on personality risks, sexual orientation or religious preferences determined by profiling.<sup>59</sup> This kind of linkage would not be possible if one's actions on the Internet were truly anonymous.

The consequences of losing one's anonymity by profiling were at issue with the United States' Total Information Awareness (TIA) program, which was cancelled after much controversy in September 2003. TIA aimed to combat terrorist risk by collecting as much profiling information as possible from "corporate, medical, retail, educational, travel, telephone" and biometric sources and then "using computer algorithms and human analysis" to detect potential terrorist activity.<sup>60</sup> According to EPIC the program was intended to create an unparalleled database of information about both U.S. citizens and foreigners<sup>61</sup> Critics argued that, TIA would chill freedom of expression as citizens became aware that their information is being recorded, and have implications for travel and employment if the information is accessed. The criticism over civil liberty and privacy issues were what caused the program to be stalled and ultimately cancelled by Congress.<sup>62</sup> The demise of TIA does not necessarily signal the end of other U.S. government profiling initiatives that are similar to TIA. Projects such as the Novel Intelligence from Massive Data within the Intelligence Community Advanced Research and Development Activity (ARDA) and CAPPS II will apparently move forward.<sup>63</sup>

## **B. The Mainstreaming of our Behaviour**

What happens to people when they realize their every transaction is being profiled and

---

<sup>59</sup> "Examined Lives", *supra* note 32 at 1398.

<sup>60</sup> *Total Information Awareness (TIA)*, online: Electronic Privacy Information Center (EPIC) <http://www.epic.org/privacy/profiling/tia/default.html> (last modified: 4 April 2003).

<sup>61</sup> "Surveillance Nation Part I", *supra* note 4 at 39

<sup>62</sup> United States, Senate, Amendment No. 59 (23 January 2003) at S1413. < <http://www.epic.org/privacy/profiling/tia/sa59.html>> (date accessed: 27 April 2003).

<sup>63</sup> ARDA, "Novel Intelligence from Massive Data at [http://ic-arda.org/Novel\\_Intelligence/index.html](http://ic-arda.org/Novel_Intelligence/index.html). (date accessed: 15 September 2003). See generally Passenger Profiling, online: Electronic Privacy Information Center (EPIC), <http://www.epic.org/privacy/airtravel/profiling.html> (date accessed: 15 September 2003).

they have lost anonymity in their online activities ? Do they change the way they behave? Or do they continue behaving the same way? Critics argue that with increased profiling “individuals will tend to gravitate towards a safe average, suppressing their individuality and creativity in favour of a thorough orientation to the demands of an omniscient observer”<sup>64</sup> I am similarly arguing that in a world of identifying technologies, our lost anonymity will cause a chilling effect where people may be scared to read or listen to materials that are controversial or stigmatic for fear that their visit is recorded. For example, it will chill our desire to visit non-mainstream sites like alternative politics, (as in our second scenario), and will also make us think twice about looking for information on stigmatic topics such as incest, aids and sexual orientation. As well, with increased restrictions on intellectual property use through either copyright management systems, geo-location technology or Ranger-type anti-infringement surveillance, people may be weary of trying new material at all; for example, not bothering to listen to a music clip from a new band’s website because they do not want to identify themselves before gaining access. Cohen reasons that the “practical effect [of these technologies] is to diminish the freedom of purchasers to use intellectual products as they wish.”<sup>65</sup>

Roger Clarke asks us to consider the effect of such a society on “religious and cultural minorities, persons-at-risk, the formation of opinions, political expression, creativity in the arts, [and] innovation in business and industry”.<sup>66</sup> Effects in these areas can already be seen in authoritarian countries such as China and Burma where dissident Internet content is often

---

<sup>64</sup> Phillip Agre and Christine Harbs qtd in David Brin, *The Transparent Society*, (Reading: Addison-Wesley, 1998) at 298.

<sup>65</sup> “Examined Lives”, *supra* note 32 at 1385. A current example of the effect of monitoring on intellectual products is the substantial decrease in file-sharing in the U.S. since the RIAA started monitoring file sharing networks and suing users. File sharers are worried that their downloading and sharing activities will be monitored and then used against them which is a desired outcome for the RIAA.

<sup>66</sup> Roger Clarke, “Beyond the Alligators of 21/12/2001 There's a Public Policy Swamp” (Privacy.au, Sydney, 24 October 2001), online: <[http:// www.anu.edu.au/people/Roger.Clarke/DV/PPSwamp.ppt](http://www.anu.edu.au/people/Roger.Clarke/DV/PPSwamp.ppt)> (last accessed: 27 April 2003).

checked for fear that it will gain unwanted attention and punishment from authorities. A good example of this is the Chinese persecution of followers of the Falun Gong spiritual movement; the Chinese Internet police monitor Internet cafes, chat sites and popular web portals in order to identify and punish anyone who advocates the movement on the Internet.<sup>67</sup>

Although authoritarian states are not representative of what happens in democratic ones, they do present us with an extreme example of what can happen if the profiling of our actions becomes the norm. With no anonymity, it is less likely that we will make choices that single us out. Cohen writes that the “pervasive monitoring of every first move or false start will, at the margin, incline choices towards the bland and the mainstream.” Weinberg agrees, arguing that trusted systems will facilitate and increase the monitoring of individual thought.<sup>68</sup>

Attention should also be given to the effect of offline identifying technologies on the mainstreaming of actions. For example, U.S wireless carriers intend to have precise location reporting available for cell phones that pinpoints its location and shows the “‘bread crumbs,’ or any number of places a cell phone has been in the last few hours”.<sup>69</sup> How will such geo-location technology affect our actions? Will we modify our behaviour if we know that our location is identifiable by anyone who pays for the service? I believe that we will. The simple example of the third scenario, a philandering husband who knows his wife can check on his location at any time, demonstrates that behavioural modification will be the likely consequence of an increase in consumer use of identifying technologies.<sup>70</sup>

---

<sup>67</sup> Amnesty International, “People’s Republic of China: State Control of the Internet” online: [http://web.amnesty.org/web/content.nsf/pages/gbr\\_china\\_internet](http://web.amnesty.org/web/content.nsf/pages/gbr_china_internet) (date accessed: 27 April 2003).

<sup>68</sup> “Hardware-Based ID”, *supra* note 1 at 1269, 1270.

<sup>69</sup> Ben Charny, “Can geo-location services find the way?” *CNET News.com* (10 March 2003), online: [News.com http://news.com.com/2100-1039-991681.html](http://news.com.com/2100-1039-991681.html) (date accessed: 29 April, 2003).

<sup>70</sup> It should be noted that there are optimists who argue that behavioural modification will not occur. For example, Esther Dyson believes that we will come to a point where people will feel comfortable having their every move recorded, and will not feel the need to modify their behaviour because of it. According to her “[people] will no

### C. Self-regulation by Corporations

Another implication of identifying technology being widely used is the increase in self-regulation by corporations that will occur through the ability to identify individuals' activities. As the example of the RIAA and the MPAA have shown, corporations are increasingly substituting the traditional regulatory power of authorities, for their own in-house responses to their grievances. Although private actors have always had the ability of hiring private investigators, technology such as Ranger now allows self regulation on an unprecedented scale.

A good example of the dangers of self-regulation is the 2001 Acme Rent-a-Car case, where a car rental company used GPS satellites to track customers' speed and automatically fined them for each speeding infraction.<sup>71</sup> After a public outcry against Acme's actions, the Connecticut Consumer Protection Agency ordered Acme to stop charging fines for speeding and ask for consent from customers for any GPS tracking activities. Although the consumer protection agency and public pressure was able to halt Acme's activities, this quasi-policing role for corporations sets a dangerous precedent.

I believe that this type of corporate behaviour will only increase, whether outlawed or not, because corporations will want to be able to regulate and punish improper use of their goods, without having to resort to an inefficient and expensive court process. This will affect our ability to be anonymous as it will be in the corporation's interest to disallow unidentifiable transactions because it will not be able to control them. The technology will increasingly dictate how we are regulated, and it will be corporations, not government that will be leading the path towards new forms of regulation. Weinberg fears that since identification technologies are not limited to

---

longer feel uncomfortable being on display, since everyone around them is on display too." (Esther Dyson, *Release 2.0* (New York: Broadway Books, 1997) qtd in Brin, *supra* note 64 at 157).

<sup>71</sup> Richard Stenger, "Rental driver finds Big Brother over shoulder" *CNN* (22 June 2001), online: <http://www.cnn.com/2001/TECH/ptech/06/22/gps.airiq/> (date accessed: 27 April 2003).

legitimate governmental uses, we are “at the mercy of the casual commercial observer.”<sup>72</sup> Brin agrees, suggesting that perhaps it will be “Corporate America” rather than government that will lead us to a surveillance society where our every action is known.<sup>73</sup>

Questioning a corporation’s right to self-regulate and police will be important in an era where new technologies will make it so easy for non-governmental parties to identify us and limit our individual rights. As EPIC has argued, we must make sure that “the power to authorize policing and adjudicate guilt or innocence” does not lie with corporations, but rather remains “in the courts”.<sup>74</sup> The increase in corporate self-regulation, along with rising consumer profiling and mainstreaming of consumer choice are serious consequences to the pervasive use of identifying technologies, and worrying both for our personal civil liberties and for the long-term consequences on our society.

## V. Are there solutions?

Unfortunately, the urge to collect personal information about people will not disappear. As David Brin puts it, the knowledge that will be gained by corporations and other data gatherers “will have a life of its own”.<sup>75</sup> He believes that if corporations are prevented by legislation from

---

<sup>72</sup>“Hardware-based ID”, *supra* note 1 at 1260.

<sup>73</sup> Brin quotes The San Jose Mercury Technology reporter Janet Rae-Dupree, as saying: “Orwell’s vision of Big Brother government was off in one major respect: Corporate America is insinuating itself into our lives more than government has” (Brin, *supra* note 64 at 202). Also “Big Brother has simply subcontracted out to corporate America” Representative Edward Markley (*Ibid.*).

<sup>74</sup> Marc Rotenberg, Open Letter to College and University Presidents, Electronic Privacy Information Center (6 November 2002), online at EPIC < <http://www.epic.org/privacy/student/p2pletter.html>> (date accessed: 27 April 2003). See also Roy Mark, “Privacy Groups Assail RIAA v. Verizon Ruling” *Internetnews.com* (25 April 2003), online: [Internetnews.com http://dc.internet.com/news/article.php/2196891](http://dc.internet.com/news/article.php/2196891) (date accessed: 29 April 2003). Another worrying trend is the power that Acts like the *DMCA* give to IP rights holders. For example, during the September 2002 Congressional hearings on “Piracy of Intellectual Property on Peer-To-Peer Networks” (since abandoned), members were seriously considering giving IP rights holders the right to disrupt P2P networks that have their content. (United States, House of Representatives, The Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, “Piracy of Intellectual Property on Peer to Peer Networks” No. 103 (26 September 2002), online: < <http://www.house.gov/judiciary/81896.PDF>> (date accessed 15 March 2003)).

<sup>75</sup> Brin, *supra* note 64 at 288.

collecting personal data, they will start collecting it under the table in data havens.<sup>76</sup> What are the options then? Are we destined for a society where anonymity is a historical concept? There are three possible solutions to the quagmire that new identifying technologies have put us in: First, creating stronger technology to allow people to remain anonymous; second, changing laws to protect a right to anonymity, and third, mechanisms that hold private actors accountable for the use and implications of identifying technologies.

### **A. The Technology Solution**

The technology solution contends that developments in privacy-enhancing technologies will remain a step ahead of the identification technology. This will allow users to thwart technology such as geo-location software, by preventing it from being able to identify or authenticate the user. In his seminal text, *Code*, Lawrence Lessig argues that “law is becoming irrelevant. The real locus of regulation is going to be code”.<sup>77</sup> Lessig’s meaning becomes clear when one looks at technology such as geo-locators in rental cars that can track speeding transgressions, geo-location software that “border” the Internet because of jurisdictional concerns over IP and other web content,<sup>78</sup> or P2P monitoring programs that identify copyright infringement. Froomkin argues that technology is the only answer to increased corporate lust after our personal information: “anonymous communication and transactions are the only techniques that are likely to allow one to control the dissemination of personal information and thus even partly realize the idea of home as a secure fortress.”<sup>79</sup>

---

<sup>76</sup> *Ibid.*

<sup>77</sup> L. Lessig, *Code and other laws of cyberspace* (New York: Basic Books, 1999).

<sup>78</sup> Michael Geist argues that the corporate trend is towards the use of geographic identification technologies to “border” the Internet because of jurisdictional concerns. (Michael Geist, “Courts poised to decide Internet ‘borders’” *The Toronto Star*, (13 January 2003)).

<sup>79</sup> “Flood Control”, *supra* note 22.

Examples of privacy enhancing technologies that allow us to combat identification technology and remain anonymous include file-swapping anonymizers, anonymous browsers, digital cash and anonymous web publishers. For example, Flyster was developed in response to P2P monitors such as Ranger. It gives anonymity to file-swappers by hiding a file swapper's IP address, thus preventing P2P monitors from identifying users.<sup>80</sup> Similarly, Freenet is software that lets users to publish and obtain information on the Internet with complete anonymity.<sup>81</sup> Anonymizer and Megaproxy are anonymous browsers that allow users to surf the web without being identified by presenting a barrier between the user and the requested website.<sup>82</sup> Invisiblog allows users to publish anonymously online through an anonymous web log.<sup>83</sup> Digital cash lets users make anonymous internet purchases, by making it impossible for anyone to link payment to payer.<sup>84</sup>

Except for Invisiblog, the examples I listed above all depend on one party to a transaction accepting the use of technologies of anonymity by the other. This means that it is really up to the host website to choose to accept the anonymous visitors. Cohen argues this point as well; she says that consumer freedom is relative because "it is the vendor who is free to decide what terms to offer in the first place".<sup>85</sup> A good example of this concept is Sony's Movielink, where, as mentioned earlier, you will not be given access to the website by using an anonymous browser, because their geo-location technology cannot assess your jurisdiction.

Similarly, technology such as digital cash and intelligent privacy agents depend on e-commerce companies permitting their use. Although trusted systems that identify users are not

---

<sup>80</sup> See "Hollywood gets tough on copying:", *supra* note 45.

<sup>81</sup> See Freenet Project, online: <http://freenetproject.org/>.

<sup>82</sup> See Megaproxy, online: <http://www.megaproxy.com>. Also Anonymizer, online: <http://www.anonymizer.com>.

<sup>83</sup> See Invisilog, online: <http://www.invisiblog.com/>.

<sup>84</sup> See generally "Digital Money". EFF, online: [http://www.eff.org/Privacy/Crypto/Digital\\_money/](http://www.eff.org/Privacy/Crypto/Digital_money/).

<sup>85</sup> "Examined Lives", *supra* note 32 at 1397

*per se* necessary if you have an anonymous payment system such as digital cash that protects from fraud, it is unlikely that many e-commerce firms will voluntarily allow anonymous technologies that give them less information about their consumer. As Brin argues, the knowledge gained by corporations through consumer transactions is too valuable to give up. Ultimately, a solution which relies solely on technological remedies to anonymity concerns will be insufficient: This is because a solution depends on constant innovation and the fact that usually both parties to a transaction have to agree to its use.

### **B. Changing the Law**

Another solution to protect ourselves from the affect identifying technologies will have on anonymity is to change the law. However, there are concerns that the laws are not developing quickly enough. According to the ACLU, “The technologies of surveillance are developing at the speed of light, but the body of law that protects us is stuck back in the Stone Age.”<sup>86</sup>

Most states do not have laws that deal directly with the effects of new identity technologies. Canada has the *Personal Information and Privacy Electronic Document Act* (PIPEDA) which prohibits the use of personal information without consent, but it does not deal with a person’s right to anonymous transactions.<sup>87</sup> The European Data Protective deals with some types of consumer profiling by granting residents the right not to have legal affects based on their aggregated personal information.<sup>88</sup> The United States does not have any *pro forma* laws that regulate anti-anonymous action, but as mentioned earlier, there are constitutional guarantees to a right to anonymity in publishing and reading. Additionally, neither Canada nor the U.S. have specific safeguards against corporate self-regulation that infringes our right to anonymity. In

---

<sup>86</sup> Jay Stanley and Barry Steinhardt, “Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society” *ACLU* (January 2003) at 15.

<sup>87</sup> *Personal Information Protection and Electronic Document Act*, S.C. 2000, c.5.

<sup>88</sup> “Examined Lives” *supra* note 32 at 1435.

Canada, there are no broad-based safeguards that make sure self regulation is done for legitimate purposes: The *Charter of Rights and Freedoms* applies only to government, not corporations, meaning the same rights on search and seizure of personal property do not apply. In the U.S., courts have held that private parties need heightened scrutiny when they try to obtain a person's identifying information.<sup>89</sup>

Academics mostly believe that because the technological conditions which have led to non-anonymous expression just recently came into existence, our rights need to be reshaped to fit the technology. According to Cohen, the laws need to be amended or interpreted to protect against technological changes that limit civil rights:

Now that digital copyright management technology has made it possible to monitor reading habits, preferences regarding political commentary, artistic tastes, to intrude to an unprecedented degree on private intellectual activity of all types-- the doctrines that protect "speech" must be reshaped to ensure that the protection they afford is not diminished.<sup>90</sup>

She argues that in the United States, the long line of constitutional cases that have pro-anonymity holdings signal that the government should create legislation to protect one's right to read anonymously.<sup>91</sup> In the case of consumer profiling, Cohen believes that the solution lies in creating laws that protect informational privacy: "[N]ear impermeable barriers" should be erected "against aggregation, disclosure, use, and retention of identifying information for any purpose other than... expressly and specifically authorized."<sup>92</sup> Lessig argues the same point, stating that restrictions need to be created on the way transaction data is used. According to him

---

<sup>89</sup> See generally Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" (2002) 75 *S. Cal. L. Rev.* 1083.

<sup>90</sup> "A Right to Read", *supra* note 30 at 1015.

<sup>91</sup> *Ibid.*

<sup>92</sup> *Ibid.*, at 1037.

“you’d want to have a situation like ... credit reports—we can see them, and know something about who is using them and why, and potentially remove any errors.”<sup>93</sup>

Marc Rotenberg is optimistic that the law will invariably catch up to technology. He says that historically privacy laws in the United States “have invariably come about in response to new technologies and new commercial practices”. The examples of the telephone, video tape rentals and computer databases show that “the American tradition is to establish a right of privacy in law to enable the development of new commercial services.”<sup>94</sup> Litman is not so optimistic; she argues that such laws “are unenactable as a political matter.”<sup>95</sup> Clarke concurs, according to him “the only means whereby people can sustain privacy protections, and with it their humanity, is through 'eternal vigilance', and hard-nosed lobbying.”<sup>96</sup>

The fact that neither Canada nor the U.S. have comprehensive laws that protect citizens from the consequences of identifying technologies is worrisome. However, it is encouraging that there are on-going academic debates over how to protect civil rights in the face of changing technology. These debates underscore how important it is that policy makers create strategies that best balance the benefits of these technologies, as tools for authentication and locatability, with legitimate and equally compelling rights, such as anonymity.

### **C. Accountability through government and civil society**

Whether the problem is the lack of political will to enact laws or that the law simply cannot keep up with the pace of technological development, it is evident that there needs to be mechanisms beyond the law that force the use of identification technology to be accountable. I

---

<sup>93</sup> Laurence Lessig qtd. in D. Farmer & C. Mann, “Surveillance Nation Part II” *Technology Review* (May 2003).

<sup>94</sup> Mark Rotenberg, Submission to Subcommittee on Commerce, Trade, and Consumer Protection Hearing, “Privacy in the Commercial World” (1 March 2001).

<sup>95</sup> Litman, *supra* note 30 at 1287. Litman is pessimistic about any current solutions to the privacy dilemma: “Self-regulation is an abject failure; meaningful privacy regulation appears to be unenactable as a political matter; and accepting that privacy is an outmoded notion from a bygone age seems unacceptable.”

<sup>96</sup> “Introduction to Dataveillance”, *supra* note 2.

define accountable as meaning being respectful of how technologies infringe people's rights, including the right to act anonymously; the effect of mistakes made by these technologies; and the broad long-term societal consequences of their use. For example, Mann and Farmer questioned the consequences of mistakes in the Total Information Awareness program: "A 99 percent hit rate is great for advertising... but terrible for spotting terrorism."<sup>97</sup> They believe that in a society filled with identifying technologies, a lack of accountability on the part of the corporations and governments using these technologies is a critical issue.<sup>98</sup> It is hard not to concur.

According to David Brin, accountability is the only viable solution to the oncoming surveillance society. He argues that the idea of privacy as we know it will become outmoded in a society where government, corporations and others increasingly want complete knowledge about citizens. Instead, he believes we should strive for a transparent society that is accountable to all participants.<sup>99</sup> Brin argues that strong, yet accountable governments are the key to promoting personal freedom and constraining injustices to the people:<sup>100</sup> Governments need to be strong in order to "stave off other dangers".<sup>101</sup>

But what does accountability by corporations really mean? What sort of accountability mechanisms are we talking about? Accountability could consist of law makers defining principles that support the type of relationships consumers wish to have with corporations and marketers, as well as measures, legal or otherwise, to promote and enforce use of these principles. To this end, Clarke sets out a list of accountability principles for the use of identification technologies, such as "apply[ing] identification only where it's justified" and

---

<sup>97</sup> Mann and Farmer, *supra* note 4 at 40.

<sup>98</sup> "Surveillance Nation Part II", *supra* note 93.

<sup>99</sup> Brin, *supra* note 64 at 334.

<sup>100</sup> *Ibid.*, at 198.

<sup>101</sup> *Ibid.*

“recognize[ing] and us[ing] pseudonymity”<sup>102</sup> Brin doesn’t give any concrete solutions to what he means as accountability, although he believes that government bureaucracy is a key component to any possible solution, combined with new methods that supplement it.<sup>103</sup>

Accountability through citizen, government and non profit actions and watchdog groups can also be effective. We saw it succeed in the Real Network example, where the GUID system that transmitted to Real Networks information about music stored on a user’s computer, was pulled by the company after a public outcry. Similarly, Doubleclick put plans on hold to link its geo-location database with the buyer information database of its subsidiary Abacus after intense criticism from several state attorneys general, the U.S. Federal Trade Commission and most vocally, an irate public. After a class action suit over its privacy practices, Doubleclick settled in 2002 agreeing to give consumers access to their online profiles, verifying its compliance with the agreement, and paying \$450,000 for legal fees and consumer education.<sup>104</sup> In the long term, it is in the public’s interest to make sure there are civil society actors willing to monitor and flag improper use of identifying technologies.

## VI. Conclusion

This essay has argued that anonymity is a vital right which society can no longer be complacent about. Anonymity is a state where a person cannot be located, identified or authenticated; where transactions cannot be associated with any particular individual. Anonymity is valuable not just in the abstract, but also in terms of how its absence or presence will structure the society we live in. Being anonymous allows people to enjoy the fundamental freedoms that

---

<sup>102</sup> Roger Clarke, “Authentication Technologies and Their Privacy Implications: Technology and Policy Foundations” (National Academy of Sciences, Washington DC, 3-4 October 2001) [unpublished] online: <<http://www.anu.edu.au/people/Roger.Clarke/II/NASATPI01.ppt>> (date accessed: 1 May 2003).

<sup>103</sup> *Ibid.*, at 252.

<sup>104</sup> Office of the New York State Attorney General, Press Release “Major Online Advertiser Agrees To Privacy Standards For Online Tracking” (26 March 2002) online: [http://www.oag.state.ny.us/press/2002/aug/aug26a\\_02.html](http://www.oag.state.ny.us/press/2002/aug/aug26a_02.html) (last accessed: 1 April 2003).

are at the core of our present-day interaction with society. These freedoms include, *inter alia*, to read and publish without being recorded, to search for information without being stigmatized, and to discuss without being identified. Of course, there are legitimate reasons why anonymity should be limited, including the fact that it can, in a sense, “contribute” to illegal activity (such as music piracy) and other anti-social behaviours. However, the constructive purpose of anonymity, as a tool for freedom of expression and action, has been recognized at law as deserving of protection. Like every legal matter, it is a matter of balancing competing rights or interests.

I next argued that technologies which were the subject only of fertile imaginations, have now become commercial goods with applications for consumers and corporations. The objective of these technologies is to identify users and track their activities. To identify users, these technologies depend on sophisticated database analysis in the Internet context, or on the global reach of GPS for offline purposes. More importantly, they depend on society’s acquiescent move toward an identification and monitoring society, as the technologies become integrated into our daily lives.<sup>105</sup>

Some of the implications of these technologies are pervasive - the ability to track our activities can lead to profiling, where data mining companies can collect our transactional information to come up with a digital rendition of us, based on the sum of our transactions, reflecting our likes, dislikes and actions. Knowing that our transactions are recorded can also lead to the mainstreaming of our behaviour, where we censor our expression and gravitate to the safety of the middle in order to prevent adverse consequences. The effects of an identification society can already be seen in an extreme manner in authoritarian states, where people modify their behaviour in order to avoid unwanted attention. Another implication of the widespread use

---

<sup>105</sup> According to Mann and Farmer, “Many if not most of today’s surveillance networks were set up by government and big business, but in years to come individuals and small organizations will set the pace of growth.” (Mann and Farmer, *supra* note 4 at 38).

of identifying technologies will be an increase in self-regulation by corporations. I argued that corporations will seize the chance to regulate and punish improper use of their goods, without having to resort to an inefficient and expensive court process. Ultimately, I concluded that our ability to be anonymous is doomed to be eclipsed by geo-location technology, digital rights management systems, and Ranger-like software systems that will do their best to control the use of what corporations consider to be their property.

The question now becomes: to what extent can society move towards the use of identifying technologies, without unduly hindering legitimate legal rights to anonymity? What types of solutions are available to prevent circumstances such as my scenarios in the introduction suggest? There are options: For example, policy makers could structure an anonymity test so that no anonymity is the default rule, and consumers would have to negotiate towards individual contracts with corporations and marketers to secure their anonymity. But as Cohen has pointed out in Section III, this option is not so efficient from a transactional costs point of view, and practically-speaking, it depends on the goodwill of both parties to participate in the scheme for it to work. At the end of the day there isn't one prefabricated answer the law could ever pronounce; any test conceivable would have to be fact dependent.

Whether the problem is the lack of political will to enact laws or that the law simply cannot keep up with the pace of technological development, it is evident that there needs to be mechanisms beyond law that force the use of identification technology to be accountable. The accountability option is a viable solution to counter the effects that new technologies are having on anonymity. Unlike technology optimists, I do not believe that relying solely on technology is the answer. Technological solutions that allow anonymity will either be stymied by transactional systems that simply do not accept them, or alternatively be constantly outwitted by identity

technologies that defeat them. However, forcing corporations to be accountable could help prevent or at least stave off the implications of lost anonymity described in Part IV. Since we are dealing with competing rights of corporations and individuals, no single instrument will be enough to protect our right to be anonymous – only through a combination of law, technology and accountability will an appropriately balanced solution be found.