2016

Information Ethics: Privacy, Metadata, and the Online Profile

APPLIED ETHICS- PHIL 330

MICHAEL PINDER

Philosophical discussion regarding the practical utility of privacy has a long and well documented history. Traditional conceptions of privacy often are intimately connected with the idea of a private household, and these traditional ideas of privacy are pervasive even in a modern context. In reference to his controversial 1967 Omnibus bill, Pierre Trudeau famously told the CBC "The State Has No Place in the Bedrooms of the Nation". This notion of household based privacy has been present in the western world for more than two-thousand years. In *Politics*, Aristotle extensively discusses the separate spheres of oikos (the home) and polis (the political community).[1] Aristotle valued the separation between public and private affairs, since he valued not only private property the plurality of opinions within a state. His warning is explicit: "There can be too much unity within a state".[2] Aristotle's conception of privacy has served us well in many contexts, but it is wholly inadequate to deal with issues of privacy in the digital age. Actions taken online from the comfort of our own homes can involve nearly simultaneous communication with servers which could be halfway around the globe. In this context, privacy which is at least partially defined by spatial constraints is dated and ineffective.

In addition, recent trends regarding the collection and dissemination of user data online give especially great cause for ethical concern. In some cases, consumers are deceived and manipulated into contracts for which they are unable to offer informed consent. In others they are monitored surreptitiously without any form of consent. While both corporate and state actors claim to act according to the public interest, analysis indicates that their data collection significantly infringes on civil liberties.

[1] http://plato.stanford.edu/entries/privacy/#His
[2] Aristotle, Translation by McKeon, R. (2001). The basic works of Aristotle. New York: Modern Library.

Historical Conceptions of Privacy

Many, but not all, historical conceptions of privacy consider the family as the fundamental unit. Later discussions of privacy, especially during the nineteenth century, were framed in terms of individual property rights. According to Warren and Brandeis, by the late 1800's, the term "property" had expanded to cover not only tangible forms of possession but also intangible forms.[3] Out of this rose laws against excessive noise and odor, and, importantly, intellectual property laws, as well as laws against slander and libel. Intellectual property laws are a consequence of the conception of certain *ideas* as private property. Likewise, laws against slander and libel result from the conception of an individual's *reputation* as an aspect of private property. This expansion of property rights to include intangible assets results in a private sphere much broader than the Aristotelian conception. For Aristotle, the reputation of an individual was a public affair, and a valid ground for discontent throughout the community, whose members could assert an interest in the behaviour of others. From the nineteenth century onward however, with an individual's reputation and ideas being considered part of his/her private property, privacy expectations expanded accordingly.

During the nineteenth century, even while rights to privacy were being expanded in a legal context, there was fear that technological advances threatened our conceptions of privacy. "Instantaneous photographs and newspaper enterprise", wrote Warren and Brandeis, "have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be

[3] Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193.

proclaimed from the house-tops."[4] Despite worries of this nature being a part of the public dialogue for more than a century, ethical issues relating to privacy have not yet been satisfactorily resolved. To complicate matters, the dizzying pace of technological progress has introduced additional problems which are fundamentally different than those faced in the past.

Online Privacy

The invention of the internet was enormously significant for a multitude of reasons. It greatly facilitated globalization, and enabled the expansion of our personal spheres like few inventions before it. Friends and family could maintain connections from almost anywhere on earth, knowledge which might otherwise have remained in private libraries and universities became publicly available, and businesses could decentralize and easily serve markets remotely. This method of social interaction was so radically new that previous notions of privacy were difficult to apply. Daniel Palmer argues that this is because twentieth century conceptions of privacy, both in law and philosophy, are delineated by physical access to persons and property.

> In the past… it was largely assumed that individuals had the ability to control the access that others had to them through assuring them control over their physical self and possessions. Since physical violations of space or control are fairly transparent, the proper limits between individuals were fairly well demarcated and the ethical norms governing relationships were derived from these distinctions.[5]

If we entertain the view that an individual's reputation is indeed a part of his/her private property, it might be tempting to include all of an individual's online data as a sub-category of reputation. We could extend the domain of privacy over this new frontier, and include

[4] Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193.
[5] Palmer, D. E. (2005). Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices. Journal of Business Ethics, 58(1-3), 271-280.

ownership of online data as simply ownership of another non-tangible asset. However, because the internet necessarily involves an exchange of data between a user and a server, we must allow for a certain amount of data access on the part of websites, ISP's, etc. A better criterion than including all personal data as private property might be to allow access to data which is *necessary* for the ordinary use of web based services, but to ensure as much as possible that the data be anonymized.

Online Profiles: Rise of the Profile

Before discussing the many implications of online profiles, it might be useful to examine the way data is transferred online and clarify technical terms. Each device connected to the internet is given a unique identifying number called an IP address. In order to connect to a website, a user inputs the domain name of a website. Since computers functionally define network addresses as IP numbers and not domain names, a DNS (domain name system) request is sent to translate the domain name into an IP address.[6] Starting from the user's computer, (or client side,) data requests are generally sent through a wireless networking card to a router, then through underground cables to an ISP (internet service provider). Next, the data is relayed to a regional network hub, and, from there, to a domain name server. A *server* is a computer connected to the internet for the purpose of hosting rather than requesting data. Then the IP address of the requested website is returned and the user's device connects through as few hubs as possible in order to reach the requested IP, and return data from it. Commonly, data criss-crosses a continent, sometimes an ocean. In principle, data can be intercepted at any one

[6] Connolly, R., & Hoar, R. (2015). Fundamentals of web development. Upper Saddle River, NJ: Pearson Education.

of these points. Most requested IPs point to dedicated servers, but it is also possible to have direct peer-to-peer connections where computers act as both clients and servers.

In such a system, expectations of total privacy are difficult. One might think that privacy is lost in the first step, as soon as users are demarcated with an IP address. But it is important to make a distinction from data of the kind which is necessary for the process described above and data which is personal in nature. An IP address, in and of itself, does not contain personal information. I will use the term *system data* in this paper to refer to all data which is necessary to facilitate communication between devices and servers. I will use the term *user data* to refer to (non-anonymous) aggregated data regarding a particular user.

In the early days of the internet, users enjoyed a high degree of anonymity. People were generally conscious enough to use screennames, to not offer personal details such as location, age, or employment information. If user data was stored at all, it was either storied client-side as cookies (small pieces of data containing a saved state) or server-side by parties which the user was engaged with directly. In the early days of the internet, local server-side storage of user data "was the de facto standard for Web applications."[7] It should be noted that the purpose of this data was, in many cases, innocuous. One of the early motivations for storing user data was the ability to enable users a customized experience; allowing, for example, users to change superficial details of the layout, background or color scheme.

Today however, online profiles composed of user data are either a mandatory or encouraged aspect of most websites. The rise of the online profile would be less concerning if it was limited to individual websites keeping track of user's posts, preferences and past use of the

[7] Obrenovic, Z., & Haak, B. D. (2012). Integrating User Customization and Authentication: The Identity Crisis. IEEE Security & Privacy, 10(5), 82-85.

site. But while storing user data server-side locally was once the norm, it has recently become more common for user-profiles to have both local (to the server) and *external* aspects.[8] Consider the relatively new security model where a separate third party account handles user verification. The verification is usually handled by large companies which have fairly secure networks with which customers are likely familiar. Microsoft, Google, and Facebook, all offer services like this, and using these accounts to log in to services saves the user from having to create yet another online account and password for any site which requires a profile. In doing this, consumers often paradoxically believe they are ensuring their own information security. This is because using the same password for multiple accounts is risky, and the number of online profiles an individual is connected to which require passwords can be overwhelming. However, relying on a single company for identity verification comes with its own set of problems.

It is often asserted that advertising is the bread and butter for web companies such as Google and Facebook. Scientific American wrote in 2013 that "advertising currently drives the vast majority of the Internet industry by volume of revenue"[9]. This "advertising" label is somewhat misleading. Advertising revenue does not come simply from the banner ads that appear when using an online service. A significant part of the advertising revenue comes from the value of user-data and its sale to third parties, usually data or advertising conglomerates. Raw system data is useful to tech companies, but of little concern to anyone else. On the other hand, user-profiles facilitate tracking of online activity, linking individual data elements that

[8] Obrenovic, Z., & Haak, B. D. (2012). Integrating User Customization and Authentication: The Identity Crisis. IEEE Security & Privacy, 10(5), 82-85.
[9] Fertik, M. (2013). A Tale of Two Internets. *Scientific American*, 308(2), 13-13

would otherwise be disconnected. An individual's data is far more interesting and useful for companies if it includes personal data such as demographic information, which can either be provided by the user, or simply inferred by tracking the activity of each profile.

There is a strong motivation, then, for companies such as Microsoft, Google, and Facebook, to associate all of user data with a profile, and to encourage users to provide them directly with as much personal information as possible. It is no wonder why they would want to extend each profile beyond the limits of their own websites and products to gain insight into any place where users interact online. User data has become such big business that there are even sites that facilitate the direct sale of data from individuals themselves, without involving any "middle man" (https://datacoup.com).

Online Profiles: Targeted advertisements and Market Research

User data is so much more valuable than system data because it enables both market research on the broadest scale imaginable and targeted advertisements which directly access any niche market likely to buy a product. Companies will often make the claim that targeted advertisements are mutually beneficial to the consumer and the advertiser. However, the relationship between companies collecting data and users whose data is collected is uneven. In many cases, users are either unaware that their data is being collected, or unaware that they are being shown targeted advertisements, or both. An objection on the part of advertisers that they are acting in a user's best interest, even though he/she may not have consented, is out of place here. The relationship between the consumer and advertiser is one of capitalist industry,

not paternalistic stewardship, and any relationship between the two is governed by agreement and contract rather than civil obligation.

An agreement governing the collection and eventual sale of user data can only be construed as legitimate if the user is able to offer informed consent. If the standard of informed consent is indeed met, then there is no reason to interfere in what Warren and Brandeis might call a private sale of an individual's intangible private property. As Richard Volkman writes, "prohibiting such capitalist acts between consenting adults is paternalistic and immoral".[10] However, if the user is unable to offer informed consent, the collection and amalgamation of user data represents a predatory relationship on the part of the collecting party. In most cases, *user agreements* are offered as the standard of informed consent by the industry.

User agreements

There are two main problems with user agreements, in their current formulation, as the standard for informed consent. The first is that, in some cases, users are *assumed* to have agreed to terms and conditions simply by visiting a webpage or using a service. Such "implicit consent" is an idea with philosophical precedent. In his writings on political authority, John Locke expressed that any legitimate government *requires* consent of the populous. To avoid the problem that many citizens living under supposedly reputable governments have not given consent, Locke appealed to the notion of "tacit consent".

Locke argued that living on the land, owning property, using the public roads, etc. constitutes tacit consent; which is just as legitimate as express consent. This is a controversial

[10] Volkman, R. (2003). Privacy as life, liberty, property. Ethics and Information Technology, 5(4), 199-210.

doctrine, and rightly so, since it entails that a person can give consent without knowing that he/she has done so. In the context of a contract between two parties, it is clearly preferable that the terms of agreement be made explicit. Any appeal to tacit consent is tantamount to an admission that consent has not been acquired.

Even if one is willing to entertain Locke's notion of tacit consent in the context of online privacy, in order for such "implicit contracts" to be valid, an alternative course of action must be available to the parties involved. That is to say, the user should have the real and practical ability to either agree or not agree. Given the increasing integration of the internet into our lives, and especially into the sphere of the workplace, the option of "opting-out" is becoming increasingly difficult. If one is unable to earn a living without internet access, which is true for a significant amount of people, then it is not legitimate to claim that a person is offering tacit consent by simply using the service. The reality is simply that there is no other choice.

The second major problem with user agreements is that, even when they are provided to users, they are presented in such a way as to be largely unintelligible. The language is often opaque and torturously legalistic, presented both in fine print and in unnecessarily long form. In web based apps, user agreements are often inserted into an inconspicuous section of the installation process. All of these techniques are used to actively discourage users from reading the agreements. The end result is that users are usually unaware of the implications of user agreements that they endorse.

Christian Fuchs, a professor at the University of Westminster, published a case study which saw users of German social networking platform studyVZ tested on their knowledge of the sites

privacy policies. This topic is "framed by the context of electronic surveillance"[11]; since studyVZ had recently changed their privacy policy to allow for targeted advertisements at the time of the research. The study itself considered three main questions:

- How knowledgeable are students about the rise of a surveillance society?
- How critical are students of the rise of a surveillance society?
- How do the degree of knowledge about surveillance and the degree of critical consciousness on surveillance influence the usage of studiVZ?[12]

Users of the site were provided an online questionnaire consisting of both multiple choice and open ended questions. Results of the study indicate two important observations. The first is that users of studiVZ are generally quite concerned about information privacy. About 73% of users disagree with the statement "one need not be afraid of surveillance if one has nothing to hide" and about 87% agree or strongly agree that "corporations have great interest in gathering personal data".[13] The second is that despite the level of apparent concern over information privacy, only about 13% read the terms and conditions of social networking sites enough to meet a non-superficial standard.[14] Despite being somewhat knowledgeable and critical about the rise of a "surveillance society", many users are unaware of specific legal issues and surveillance parameters.

[11] Fuchs, C. (2010). StudiVZ: Social networking in the surveillance society. Ethics and Information Technology, 12(2), 171-185.
[12] Fuchs, C. (2010). StudiVZ: Social networking in the surveillance society. Ethics and Information Technology, 12(2), 171-185.
[13] Fuchs, C. (2010). StudiVZ: Social networking in the surveillance society. Ethics and Information Technology, 12(2), 171-185.
[14] Fuchs, C. (2010). StudiVZ: Social networking in the surveillance society. Ethics and Information Technology, 12(2), 171-185.

While a significant level of public awareness regarding online privacy issues is encouraging, the results of this study show that the public does not have a meaningful awareness of the specifics of user agreements. In the words of the study's author, "Our study indicates that students are critical of surveillance in general, although they do not have much concrete knowledge about actual surveillance policies."[15] Evidence such as this, which indicates users are unaware of the specifics of user agreements, function as evidence that the standard of informed consent has not been met. The expected rebuttal that an opportunity has been given for the consumer to be informed is disingenuous. The relevant information is commonly obscured to the point where consumers cannot reasonably be expected to be informed. User agreements serve simply as a moral smoke-screen to obscure the nature of the relationship between the subjects, and the owners, of user data.

Third party access: Data conglomerates

One of the most troubling sections commonly included in a terms of service agreement concerns the sharing of user data with third-parties. Since the sharing of data with third parties is such a contentious issue, but the data in question is so valuable, it is no small feat to dissect the truth of third party data sales. Facebook outlines its policy regarding the sale of user data to third parties as follows:

Sharing With Third-Party Partners and Customers

We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world.

[15] Fuchs, C. (2010). StudiVZ: Social networking in the surveillance society. Ethics and Information Technology, 12(2), 171-185.

Here are the types of third parties we can share information with about you:

- **Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).** We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.

  Please review your advertising preferences to understand why you're seeing a particular ad on Facebook. You can adjust your ad preferences if you want to control and manage your ad experience on Facebook.

- **Vendors, service providers and other partners.** We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.[16]

This policy seems to indicate a concerted effort by Facebook to anonymize user data that is sold for advertising purposes to third parties. Presuming that Facebook is complying with its own terms, there is still a diffusion of responsibility that happens after the sale of data to a third party. Once data is passed along, it is functionally impossible for the second party, Facebook in this case, to determine how the data will be used. It is possible, for example, for the data to be reattached to personal information even if it has initially been anonymized. While a clause can be included which prohibits such aggregation, it would be exceedingly difficult to enforce. This allows the second party to wash its hands of responsibility while still retaining the value of its profile data.

[16] https://www.facebook.com/full_data_use_policy

Within the previous paragraph it was assumed that Facebook is complying with the terms and conditions outlined on the site. However, court proceedings have given users good reason to suspect that they are being deceived by Facebook. In 2011, Facebook settled charges of misleading/deceptive conduct brought forward by the FTC.[17] The fifth count of the FTC's eight count complaint dealt with the sale of personalized data to advertisers. The FTC found that despite Facebook's promises of anonymizing advertising data, it was in fact involved in selling personal information to advertisers. The final paragraphs of count five read as follows: "Facebook has represented, expressly or by implication, that Facebook does not provide advertisers with information about its users. In truth and in fact… the representation set forth in Paragraph 41 constitutes a false or misleading representation."[18]

While this is certainly an interesting case study about online privacy, it should be noted that a business model based on the sale of user data is not unique to Facebook. Google, one of their major competitors, has been the subject of four different FTC complaints in the last ten years.[19] The fourth case, which also centered on privacy concerns, saw Google pay a 22.5 million dollar civil penalty, due to a violation of a settlement reached in the 2011 Google Buzz case. The penalty is to date the largest FTC penalty ever issued for violation of a commission order.[20] But even such steep penalties are unlikely to deter these enormous corporations from aggregating and selling user data. Alphabet, the parent company of Google, is the world's second most valuable public company with a market capitalization of 517.3 billion dollars (as of

[17] UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, Document 0923184. Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf
[18] UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, Document 0923184. Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf
[19] Google Buzz, Google AdMob Deal, Children's Unauthorized In-App Charges, Safari Internet Browser
[20] https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

April 12, 2016).[21] According to NADAQ Google's advertising revenues accounted for 90% of total revenues in 2015.[22] While these companies do not often offer much information about the source of their advertising revenue, it is clear that user data represents a valuable asset with enormous earning potential. It is therefore illogical to expect that these companies will self-regulate in any meaningful way. They have an interest in *appearing* to be vanguards of privacy, so as not to risk consumers abandoning their products in favor of products offered by competitors. Once that standard of appearance is met, they are obligated to focus on their primary duty, namely, maximizing profit for shareholders. They are not at all committed to act in the public interest.

Third party access: Government access

In cases where the third party is a government or government agency, there are special considerations regarding when it is acceptable to procure and amalgamate user data. State actors, unlike corporate ones, *are* generally committed to acting in the public interest. Data collection by the government is justified to the public by appealing to very real concerns of national security. After September 11, 2001, the United States government greatly expanded its data collection efforts under the Patriot Act. One of the many controversial sections of the Patriot Act is section 215, which authorizes the bulk collection of “metadata” by the National Security Agency.[23] The simplest definition of metadata is data about data. For example, the

[21] Retrieved from https://ca.finance.yahoo.com/q?s=GOOG
[22] http://www.nasdaq.com/article/why-googles-stock-has-a-higher-valuation-than-apples-aapl-cm573801
[23] One hundred Seventh Congress of the United States of America. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Retrieved from https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

references in the footnotes of this paper would qualify as metadata, since they contain information about text rather than the text itself.

The scope of the NSA's surveillance became international news when contractor Edward Snowden leaked government documents originating from the NSA. Three major programs entered the public knowledge as a result of the Snowden leaks: PRISM, XKeyscore, and Tempora. PRISM was the most widely publicised of these, although it is less ambitious in scale than the other two. It involves the cooperation of the government and major tech companies (Microsoft, Google, Yahoo, Facebook, Google, Apple) in accessing data on company servers at the government's request. XKeyscore has a very different goal; it stores content en masse into a database which is searchable in posterity. Tempora is a British intelligence program similar to XKeyscore, especially strategic given England's status as a network hub on the other side of the Atlantic. Leaked documents also list other international governments who have been assisting the NSA in intelligence efforts. In addition to the UK, Canada, Australia, and New Zealand have all been implicated as collaborators.

While corporate server data is accessed through PRISM on a case by case basis, Tempora and XKeyscore employ a dragnet collection method. This is undoubtedly a useful tool for law enforcement organizations. Leaked NSA training documents assert that over 300 terrorists have been captured using intelligence generated from XKeyscore as of 2008,[24] and examples in the training material indicate a truly staggering amount of efficiently indexed metadata. While it is important to consider the success of these programs from a national security perspective, it is not clear that the method of collection is ethically justifiable.

[24] XKeycore training presentation, retrieved from https://www.documentcloud.org/documents/743244-xkeyscore-slidedeck.html

Evidence such as the StudiVZ case study earlier discussed suggests the public is critical about the rise of a surveillance society. The nature of dragnet collection is that most of the data collected is not connected to any terrorist activity or ongoing investigation. This surveillance by default completely bypasses the ordinary safeguards of personal privacy in a democracy, such as search warrants, which exist to prevent systematic abuse of power by the government. Moreover, it grants the state access to that intangible form of property, reputation, which has long been considered a private asset.

Whether handing over this private asset to the government is worth the benefits it brings to national security is a question worthy of national debate, but the way in which these programs have been implemented has not included this dialogue with the public. Instead, in the United States, these surveillance programs were implemented through temporary “wartime” legislation, which was continually extended by successive governments. The programs were kept top secret, and when details were divulged to the public by a conscientious objector, he was persecuted by the government and forced to flee, despite widespread support from the public. All of these actions serve to indicate that major world governments are unwilling to risk dialogue with their citizens regarding these programs, fearing that they would not garner public support. As in the corporate sector, the data is simply too valuable an asset for the governments to ignore, even if it means circumventing privacy laws previously demanded by the populous as a component of civil liberties.

Conclusion

The process of technological progress necessitates revision of traditional notions. Faced with multiple unresolved issues regarding online privacy, citizens of western democracy are obligated to establish a formal position.[25] It falls on the populous to demand this; for the interests of both the state and private industry are well served by leaving the system well enough alone. If citizens do not assert their rights to retain certain intangible property it is very easily stolen from them and very difficult to recognize the theft. In the humble view of this author, approaches to the ethical issue of personalized data come in three varieties.

First, we as a society could work to ensure the widespread anonymization of user data and prevent data amalgamation. This represents a conservative position, and it would require a conscious decision not to capitalize on a very valuable asset in the name of privacy. It is conservative in that it represents a wish to return the internet to a previous era. This position would likely meet heavy opposition from both government and the private sector. In addition, even if such a position was adopted as a national policy, international cooperation would be unlikely. Those countries, and companies within them, who did not adopt such a policy, would be at a distinct competitive advantage. In addition, it would be difficult to prevent data collection on citizens by foreign entities without limiting connectivity, which itself would carry an economic cost. In short, it would be very difficult to implement, and would represent significant economic sacrifice for the sake of privacy.

[25] My focus has been on data collection in western democratic countries. The governments of these countries who have been exposed as participating in large scale data amalgamation programs have been listed above. There is some evidence of similar intelligence projects in both Russia and China, and while compelling, the difference in political climate puts these countries outside the scope of this paper.

Second, we as a society could legislate the open publication of large scale user databases. This represents a liberal position. The publication of data sets like this would facilitate open source collaborations and result in a more unified and comprehensive archive of user profiles. Philosophically, this approach represents rescinding the boundaries of privacy to include reputation *as a part of the public domain*. This is an enormous shift, and it would substantially erode our right to privacy, but an incredibly valuable asset would become publicly available. This second position represents a significant sacrifice of privacy in the interests of public knowledge.

Third, we as a society could attempt modest reforms to the current system. This represents the moderate position. In terms of advertisers and data conglomerates, this would mean setting a standard for informed consent which is reasonable, and ensuring that companies abide by their own terms. In that endeavour, government regulatory bodies should be empowered to take the necessary steps to protect their citizens. As to surveillance by government bodies, those entities which claim to act in our interests should be forced to uphold the mandate of the people. If we decide it is to our benefit to sacrifice our rights to privacy in the interests of national security, then we must sacrifice them *of our own volition*. Any user data collection program which is not approved by the democratic process represents theft of intangible private property on the part of the state.

Bibliography

Allen, A. L. (2011). Privacies Not Wanted. *Unpopular Privacy: What Must We Hide?*, 1-26. Retrieved January 24, 2016.

Aristotle, Translation by McKeon, R. (2001). The basic works of Aristotle. New York: Modern Library.

Bennet, C. J. (2011). Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology, 3*(3), 195-208. Retrieved January 24, 2016.

DeCew, J. (2013). Privacy. *Stanford Encyclopedia of Philosophy*

Fertik, M. (2013). A Tale of Two Internets. *Scientific American*, 308(2), 13-13.

Fuchs, C. (2010). StudiVZ: Social networking in the surveillance society. *Ethics and Information Technology*, 12(2), 171-185.

Mayer, J. R., & Mitchell, J. C. (2012). Third-Party Web Tracking: Policy and Technology. *2012 IEEE Symposium on Security and Privacy*.

Obrenovic, Z., & Haak, B. D. (2012). Integrating User Customization and Authentication: The Identity Crisis. *IEEE Security & Privacy*, 10(5), 82-85.

Palmer, D. E. (2005). Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices. *Journal of Business Ethics*, 58(1-3), 271-280.

Pham, C. (2014). Effectiveness of metadata information and tools applied to national security. *Library Philosophy and Practice*.

Sipior, J. C., Ward, B. T., & Rongione, N. M. (2004). Ethics of Collecting and Using Consumer Internet Data. *Information Systems Management*, 21(1), 58-66.

Tavani, H. T. (2004). Genomic Research and Data-Mining Technology: Implications for Personal Privacy and Informed Consent. *Ethics and Information Technology*, 6(1), 15-28.

United States Congress. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Retrieved from https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

United States of America Federal Trade Commission, Document 0923184. Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf

United States of America Federal Trade Commission (2012). Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser. Retrieved from https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

Volkman, R. (2003). Privacy as life, liberty, property. *Ethics and Information Technology*, 5(4), 199-210.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193.

XKeycore training presentation, retrieved from https://www.documentcloud.org/documents/743244-xkeyscore-slidedeck.html

Facebook data use policy retrieved from:

https://www.facebook.com/full_data_use_policy

Google financial data retrieved from:

https://ca.finance.yahoo.com/q?s=GOOG

http://www.nasdaq.com/article/why-googles-stock-has-a-higher-valuation-than-apples-aapl-cm573801

Broadcast date etc from Trudeau's speech retrieved from:

http://www.cbc.ca/archives/entry/omnibus-bill-theres-no-place-for-the-state-in-the-bedrooms-of-the-nation