Thank You for Participating in Our Criminology 417 Survey: Privacy and Surveillance in a Digital Age

If you are reading this then you are probably one of the people who participated in the initial test of the survey the Criminology 417 class of Fall/2020 put together regarding privacy and surveillance on the internet. Although the results from our little survey will never be published (because it was intended more as a class exercise at designing a study and involves no more than what would be considered a "convenience" sample), we nonetheless wanted to share some of the results with you as a thank you for taking the time to help us out by participating. In this report you will find:

- Some basic findings from the survey;
- Some findings from the individual projects that students conducted on an aspect of the data that interested them;
- Suggestions for what we, companies and legislators can do to better protect our privacy and personal information;
- Links throughout the report to media articles and videos that speak to the various issues we had in our survey as well as to our course web page, which contains links to many other resources in the event you would like to read or view further.

The Survey and Those Who Responded

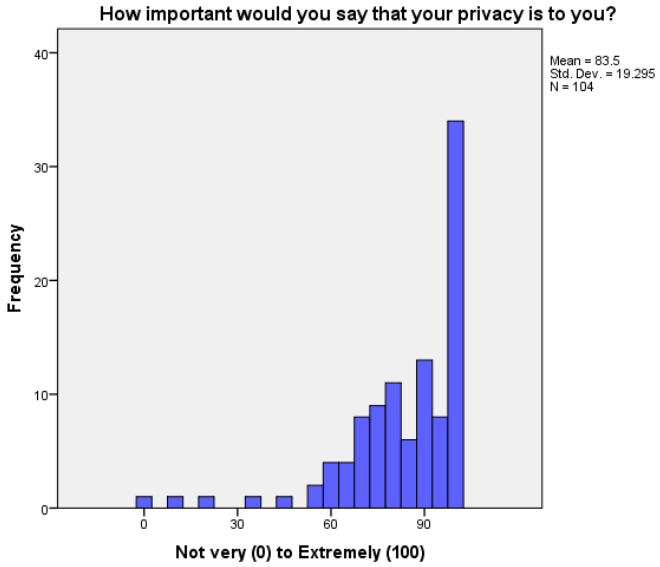
There were 13 students who took the class, and all of them contributed items for the survey, which we then organized into thematic topics and whittled down to the version that we put online in November. Each of us sent invitations to around 10 people we knew, keeping in mind that the ideal would be to get a diverse sample with respect to such attributes as age, comfort with technology, internet and social media engagement, and so on. In the end, 113 people participated in the week we had it online, which is a decent enough sample size to be able to begin doing some analysis (but keeping in mind it is a convenience sample). If you're someone who loves seeing data in more detail, feel free to check out the distributions for all the questions at https://www.surveymonkey.ca/results/SM-T623NMG67/

Some Basic Findings

We'll begin by outlining some basic descriptive information about the sample and the views that were expressed. For starters, we had some good variation in the age groupings that were involved. As might be expected, the largest number of participants were individuals around the same age as the students in the class (there were 47 people who were born in 1996 or later and thus have grown up in an internet world), but we also had reasonable numbers of people from earlier historical cohorts (13 born pre-1960; 17 born 1961-79; 23 born 1980-95). There was also good variation in how much time people spent online, and the extent to which people engaged with social media.

The Value of Privacy

Although the sample was quite diverse in many respects, there were other aspects of the results that showed much less variation. For example, one item asked people to show on a sliding scale how important privacy was to them. The numbers could range from 0-100, and 100 – the highest number on the scale – was actually the number chosen by more than a third of the people who responded. The figure at right illustrates the distribution of responses we received. It's an interesting question whether we just had a very privacy-concerned set of respondents overall, or whether the people in our sample are indicative of how much most people value their privacy. Those of us in the class came to appreciate the important role that privacy serves in our lives, and the literature we reviewed suggested that privacy is actually hugely important both for individuals and for society more generally.

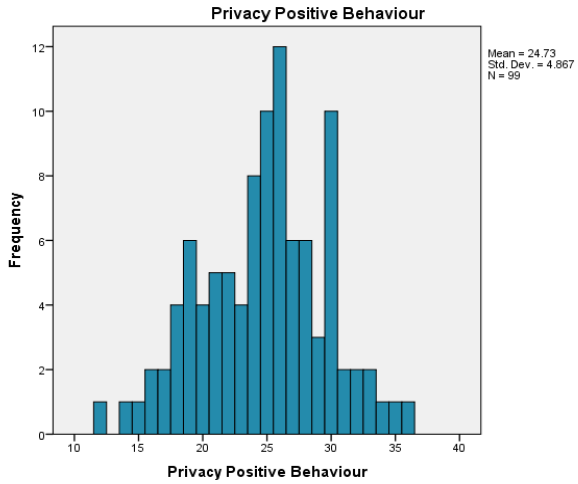


Corporate (Dis)Trust

In another question we asked how much you trusted the major internet companies, and it was also very clear that you feel the major internet companies do *not* have your interests at heart, which, as we learned in the course, is a pretty accurate view to hold. On a 1-5 scale with lower numbers indicating lower trust, the two least trusted were Facebook (with an average rating of 1.36 and where more than ¾ of those who responded indicated they do not trust the company at all) and Twitter (at 1.90). Even the two most trusted of the group – Apple (at 2.72) and Microsoft (at 2.66) – had average ratings on the "distrust" side of the scale. Perhaps most surprising to us was that Google/Alphabet rated in the middle of the pack (at 2.28). During the course we learned that Google is actually the company that launched what has become known as "surveillance capitalism" (a phrase popularized by Harvard Professor Shoshana Zuboff), and is among the most predatory in terms of the personal information it gathers, beginning with what we are thinking about at that particular moment every time we use Google Search, or Google Nest, or Google Home, or Google Anything.

Privacy-Protecting Behaviour

Another approach we took with the survey responses was to combine similarly-themed items to create larger scale totals to get a broader sense of things like how much people's concerns about privacy translated into actual behaviour when engaged with the internet. For example, we combined all the items that asked to what extent you engage in certain practices that are privacy-protecting (e.g., using a VPN; encrypting files; monitoring privacy settings) or privacy-compromising (e.g., logging into Facebook



and then connecting to other sites; "liking" things on the internet; tagging pictures with names). What we found was lots of variation among our respondents, as the graph at left illustrates.

Two related sets of questions asked about (1) your ability to do different privacy-protecting practices and (2) your desire to know about those practices. Although there was lots of variation in terms of how capable people said they were, people at every ability level indicated they wished they knew more. In class we talked about some of the things that individuals can do to better safeguard personal information, so whoever invited you to the survey may have some suggestions you can incorporate, and we'll offer other suggestions below, but one site that we recommend if you are looking for advice and techniques is the Electronic Frontier Foundation site at https://ssd.eff.org/module-categories/basics

The Student Projects You Enabled

One of the things we appreciate most about your participation is that it gave us enough data so that the students could go beyond the sort of basic descriptive information reported above to explore in more detail some aspect of the data that interested them.

Correlates of Privacy-Related Views

Chrissy tried to take more of an overall look at the correlates of concern about privacy. Keeping in mind that even the people who were less adamant about their interest in privacy still viewed it as quite important, she found that greater concern with privacy was significantly related to a number of other measures. These included (1) being much more concerned about the sensitivity of the personal information (such as contacts, search history, content of texts) that is gathered; (2) being more strongly motivated to learn how to better protect their privacy; (3) valuing privacy more strongly than sharing; (4) engaging in more privacy-protective behaviour and avoiding more privacy-compromising behaviour when online; and (5) being more adamant about the need to regulate the internet in ways that would better protect personal information.

Technophiles and Technophobes

Viktor started off by asking whether people who consider themselves technophiles (who love technology) or technophobes (who feel uncomfortable with technology) would differ in their interest in privacy and enagement in privacy-protective behaviours. Interestingly enough, he found that comfort with technology made no difference in terms of either the importance attached to privacy or engagement with privacy-protective behaviours. Whether you love or hate technology, in other words,

bears no relation to how much you value privacy or the extent to which you engage in privacy-protecting behaviour. However, privacy-protection ability does tend to be higher among technophiles than among technophobes. This suggests enhancing people's abilities by finding ways to share that knowledge/skill is clearly the way to go.

Age-Related Online Activity

Clarissa, **Sophia** and **Sarah** focused on differences between historical age groupings in terms of the concerns the different groups had about privacy, their online behaviour, and the precautions people do or don't take when they go online, and particularly when they use social media.

Sophia took a lifecycle approach to distinguish between three different age groups: (1) the youngest group who are 24 years and younger; (2) a middle group from 25 to 40; and (3) an older group who are 40+. She noted the youngest group experience more social pressure as they are deciding who they are, finding their careers, expanding relationships and possibly starting families; the mid-group are often more settled, are in their careers, paying their mortgages and perhaps raising children; and then the oldest group who are typically the most stable in their social groupings and less in need of social validation. She suggests these life cycle differences have implications for people's motivation to be online, which in turn leads them to engage in different online activities that expose them to different sets of risks. Sarah framed her analysis in terms of the "privacy paradox" – the finding in the literature that while people express concern about privacy, they nonetheless engage in all sorts of behaviours – like posting all sorts of personal information online – that would seem to show the exact opposite.

One of Sophia's key findings was that, while the older age cohort in our sample was more concerned about privacy than the younger ones, it was the youngest group who best understood how to protect their privacy. Sarah shed further light by noting that the younger group spent a significantly greater time online, and were engaged in a broader array of online activities, but were more likely to engage in privacy-protecting behaviour than their older counterpart. Clarissa pointed to similar findings.

We would add a caution here, however, because one of the things we learned in the course was how much the various internet-based companies typically do their best to make it difficult for you to exercise those controls. The "default" settings are always for disclosure, and it is not always easy to find where the controls are. The companies also use everything from the colours of buttons (e.g., Google actually tested 35 different hues of blue) to the warnings you get about potential disastrous consequences if you do not say "yes" to nudge you toward sharing (e.g., see Deceived by Design by Norwegian Company Forbrukerrådet). Two more important things to know are (1) the information you supply to companies goes far beyond what you willingly share – activity-monitoring "cameras" (e.g., pixel cookies and beacons) into your activity exist on web pages all over the internet; and (2) the information about you is incorporated into a far broader range of algorithms and broader range of purposes than those that decide what "personalized ads" you will see (see Zuboff again).

Seeking Privacy in a Surveillance Economy

Jun, **Adrienne**, **Tyler** and **Dom** focused on corporate trust and internet activity. Dom and Jun started off by trying to compare those who completely distrusted the six corporations we asked about (Google, Facebook, Twitter, Amazon, Microsoft, Apple) versus those who were higher in corporate trust, though they caution that even the "higher corporate trust" group had an average trust rating that was on the "distrust" side of the scale. Not surprisingly, the two groups differed overall in the level of privacy-protecting behaviours they engaged in, with those with the least trust being most active at that protection. The statements that most contributed to those differences involved privacy-compromising behaviour – logging into Facebook and accessing other sites through a Facebook account; allowing social media to create a news feed; and posting and tagging pictures online – which led Dom to suggest that the most effective place to focus when educating people about safeguarding privacy might be to focus on how to avoid more privacy-compromising behaviours.

Rather than deal with all six companies we asked about, Tyler and Adrienne decided to focus on the one people thought – with good reason – is the most invasive of them all, i.e., Facebook. One of the fascinating things about the data regarding Facebook was that while a full 79 people (76.7% of those who answered the question) gave Facebook the lowest possible trust rating they could, 44 of the 79 nonetheless still use Facebook. Adrienne and Tyler were interested in what explanations people might give for doing so, as well as in how they may have adapted their use of the site.

Adrienne approached her analysis by wondering what makes Facebook so compelling that people make what seems a Faustian bargain by continuing to use its services. What she found was that people who distrusted Facebook but used it anyway did so for the most part because they felt they had no choice; they saw no viable alternative and having a Facebook presence was a fundamental part of interacting in the contemporary world. As one participant she quotes said, "I don't like it, but I felt like I need to have it." Why? Many stated it was how they kept in touch with family and friends, kept track of birthdays, and/or used it to schedule events. Others said it was an important adjunct to business. But many also indicated they now read but post little if anything, and felt protected by this minimal engagement.

Tyler's analysis revealed that those who feel that way – being protected by posting little – did not seem aware of the extent to which personal information is nonetheless gathered about them by Facebook both within their account and beyond. For example, many people appear unaware that, when you log in to other accounts through Facebook, the company rides with you everywhere you go, gathering further data about you with each move you make. Also, as Tyler points out, although your privacy settings may influence who out there in the world can see what, many do not appreciate that Mark Zuckerberg sees all – even things you start to post and delete, which Facebook sees as "self-censorship" – and retains all. Readers who would like to know more about Facebook's approach might view a video interview with Roger McNamee, an early Facebook investor and insider; a well-informed analysis by journalist Carole Cadwalladr of Facebook's role in events such as Brexit and the 2016 US election can be seen in a TED talk or one of her pieces in the *Guardian*.

Why is Google Trusted More than Facebook?

Selena began her paper by noting that while approximately three quarters of our survey respondents indicated they did not trust Facebook in the least, only about 40% of respondents said the same thing about Google. Noting that this is consistent with findings from other surveys, she wondered whether that was reasonable given the activities of the two companies.

As we learned during the course, Google was the company that invented the "surveillance capitalist" model that we live with these days when we engage the internet, somewhere around the time it abandoned its original motto of "Do No Evil." Google employee Sheryl Sandberg then took herself and the Google economic model to Facebook, where Mark Zuckerberg was also looking for a way to make money.

Although both Facebook and Google subscribe to the surveillance economy, there were also differences between them in the range of information they gather. Selena concluded that while people trust Facebook less, Google is the far more pervasive collector of personal information through its search engine and myriad other services. She cautions us by noting what is called the "control paradox," i.e., the phenomenon by which people who believe they have control over their personal information tend to share more than those who believe they do not have that control. The upshot of this is that, because people seem to (erroneously) believe that Google is the more innocuous company that gives them greater control over their information, we may share more information with Google than Facebook, notwithstanding the fact that both companies deserve our caution.

Internet Concerns

Mattias looked at the concerns that survey respondents indicated when asked to indicate the "concerns or issues that come to mind when you think about your privacy online." The most common of these were concerns associated with surveillance capitalism, i.e., concern about being monitored constantly and the way that information about them is collected by third party sites who sell (or rent) that information to other companies who benefit, as well as what many people felt was government inaction in protecting their interests. If you don't already have a good sense of what information is gathered about you online, take a peek at an article from the *Guardian* where Dylan Curran shared some of what Facebook and Google had gathered about him.

Concerns about government surveillance surfaced as well, and we learned in the course these concerns are well placed, particularly if you are someone who engages in constitutionally protected activities such as non-violent protest, with those who try and assert and protect Indigenous rights and promote environmental responsibility #1 and #2 on the surveillance list. Facial recognition technologies (whose development has been aided by the name tagging that people do with their Facebook and Instagram photos) and apps that can harvest contact information and social media messaging in defined geographical areas are becoming more pervasive.

One of the things that surprised Mattias was on how little attention respondents paid to how surveillance promises to become even more pervasive as the Internet of Things becomes more

widespread. More and more products that people use – TVs, cars, baby monitors, vacuum cleaners, sex toys, refrigerators -- are internet-connected and contain sensors that gather information that is added to the pile that is known about us, leading to media reports that refer to the "Interthreat of Things." In addition to the information these products gather, authors in the area express concern that security is often minimal with these items leading to the problem that hackers can use these low-security devices as an open window that allows easy entry to your computing network to install spyware and other malware.

The Future

The course certainly raised our sensitivity about the extent to which we are being monitored wherever we go on the internet and the various ways our personal information is used. Our final class dealt with the question of "what happens next?", and we looked at three different places where protection of personal privacy can be enhanced: (1) what we can do as individuals; (2) what internet-based companies can do; and (3) what legislators can do.

What We can Do

Nothing will change in the world of Internet governance in the immediate future, which means that the first line of protection of privacy lies with us. Toward that end, one thing we can do is to vote with our feet and use other companies – particularly ones that are developed by the open source community and/or that incorporate principles of privacy-by-design – whenever alternatives are available. In that regard, we have a number of suggestions of possible alternatives and other forms of protection you can implement that will allow you to protect your personal information as well as you can given the internet as it is. In particular, we invite you to consider any of the following that you do not do or use already:

1. **Information Resource**. If you are looking for a one-stop resource with great advice on how to protect your personal information, we suggest the Electronic Frontier Foundation (EFF), who you can visit at https://www.eff.org/ We also will leave up our course web page for the next month in case you would like to see any of the articles, videos and media we read, watched and discussed during our time together: https://www.sfu.ca/~palys/crim417-2020.htm
2. **Trackers**. If you would like to know whether and to what extent you are being monitored whenever you visit a web site, and would like to exert some control over who does so, consider installing Ghostery and/or Privacy Badger as an add-on for your browser. Information about Privacy Badger can be found at https://privacybadger.org/ while information about Ghostery can be found at https://www.ghostery.com/ . Both are free – products of the open source community who operate by donation and do not collect your personal information. If you have not yet installed these, you will be shocked by how many different beacons, trackers, pixel cookies and so forth are invisibly present on almost any web page you visit.
3. **Browser**. If you are looking for a more secure browser, you might try Mozilla Firefox, another open source product. Mozilla is a company that prides itself in providing you tools that will help you protect your information when browsing the internet. See https://www.mozilla.org/en-US/firefox/new/

4. **Search Engine.** Rather than sharing your every thought with Google, try using a search engine like Duck Duck Go, which does not track you or retain your search history by default. See https://duckduckgo.com/
5. **https Everywhere**. There is a difference between web sites whose URL begins with http versus those that begin with https; that extra "s" on the end stands for "secure." Many web sites can be accessed either way, and it is always preferable to use https rather than the http version whenever you can. The Electronic Frontier Foundation has a free add-on for your browser called "https Everywhere" that will always choose the https version of a site when one is available, but still go to the http site when no "s" version exists. See https://www.eff.org/https-everywhere
6. **Email**. With programs like Facebook's Messenger or Google's Gmail, you may as well be sending a cc to each company. Google even argued in court that email was more like a post card than a letter, and hence that Google has every right to look at the content of your Gmail. If you'd like a completely secure email, check out Protonmail, a Swiss company that provides exactly that. A basic but quite functional account is available for free, or you can buy a subscription that opens more features, storage, etc. See https://protonmail.com/
7. **Encryption**. If you would like an easy-to-use encryption program to secure your files, you might check into a French company called VeraCrypt at https://www.veracrypt.fr/en/Home.html . VeraCrypt involves creating a "container" that can be any size and into which you can put any type of files. You can also encrypt entire hard drives. The software is open source and free (but open to donations).
8. **Texting/Messaging.** Instead of using the messaging app that came with your Android or iPhone, or WhatsApp (which is owned by Facebook and is about to further relax its exchange rules with the parent company), check out Signal at https://www.signal.org/

What Internet Companies Can Do

Internet companies, particularly the biggest ones that benefit most from the surveillance economy model, would have you believe that theirs is the only viable economic model for the internet, and so you should just accept it and get used to it. Shoshana Zuboff is among the many scholars and industry commentators who argue against that view, reminding us that the public internet is barely 25 years old. Zuboff suggests Silicon Valley's current frontier behaviour parallels the actions of the robber barons and industrialists who became wealthy in the late 1800s/early 1900s before the advent of child labour laws, unions, anti-trust legislation and so forth, which eventually tempered their greed and exploitation. That said, there is no incentive for the internet companies to abandon the surveillance economic model that has made their developers the wealthiest people on earth, and they benefit from our acceptance of what we are supposed to see as the "inevitability" of the current model.

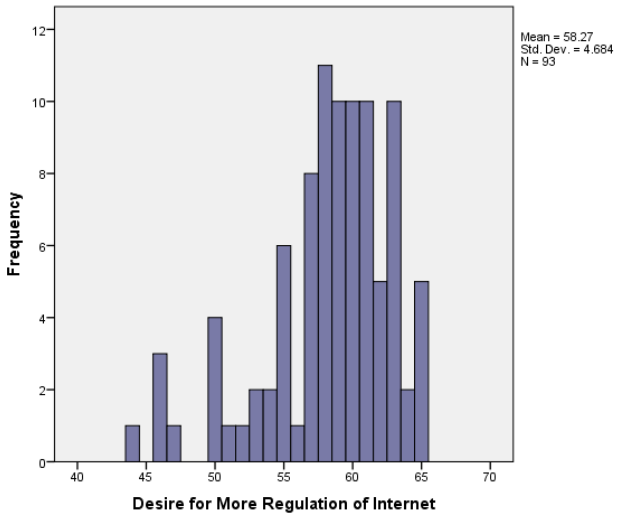
Failing more government regulation, the more people vote with their feet and show they favour companies that incorporate privacy-by-design – a set of principles that seems more broadly considered and implemented in Europe than in North America – the greater the pressure on those that remain to make customer service – where we rather than advertisers are seen as their customers -- their priority. Certainly these are key concepts we see in the open source community.

This does seem to be a time of reckoning to some degree, at least in part because of how the surveillance economy and the battle for our attention has made social media complicit with some of the great human tragedies of the last decade. Further, concern that the larger companies have become so large that they are now predatory to the point of trampling competition and stifling innovation is leading to anti-trust investigations in the United States. Facebook's apparent response – to announce a change in the WhatsApp Terms of Service to come into effect in February that will even deepen the link between the two companies – suggests the company will resist vigorously.

What Governments Can Do

Governments thus far have been enablers of the internet, with little in the way of regulatory legislation because the early emphasis was on promoting growth and innovation. Also, law is slow to catch up because so much of what we now see is unprecedented and strains old categories and concepts ... like privacy. The big internet companies have exploited that void by taking the approach that it is better to apologize than to ask permission, which is part of how companies like Facebook and Google in particular were able simply to declare by fiat that the world's information belongs to them.

A growing chorus of voices is encouraging greater regulation of the internet and its surveillance economy for the greater public good. Tim Berners-Lee, for example, who often is credited as the inventor of the world wide web, has called for this, and the UN Human Rights Council has affirmed that privacy on the internet should be considered a basic human right.



Our survey respondents would seem to agree. The graph at right shows totals on a "Desire for Regulation" scale we created by combining responses to the 14 statements in Questions 20-22 (totals could range from 14 to 70).

It is noteworthy Europe is ahead of North America in terms of having legislation – the General Data Protection Regulation (GDPR) -- which, while not perfect, nonetheless prioritizes digital privacy. What will Canada do? Ted was in Ottawa prior to the COVID outbreak, had occasion to meet with senior legal and policy advisers in the Office of the Privacy Commissioner, and was heartened to see everyone there reading Shoshana Zuboff's The Age of Surveillance Capitalism. It is also noteworthy that the Liberal Government announced in late 2020 that they would bring forth new privacy legislation for Canada in 2021, and outlined some guiding principles that appear promising. But if your privacy is important to you, as our survey gave every indication of it being, then we encourage you to monitor the legislation's progress and let your MP know your views as the discussion progresses.

A Final Few Words

This has become a bit longer than I originally intended, but the students and I wanted to convey our heartfelt thanks one last time for taking the time to help us out by participating in our survey. We learned a lot during the survey design process, and looking back on it we now see redundancies and omissions that should be fixed for the next iteration of the survey. Nonetheless, we hope this summary shows you how meaningful your participation was for the students in the course; if we shared something you didn't know already that would please us as well.

For me personally, the pervasiveness of the surveillance economic model is a great travesty because in addition to being a privacy advocate, I am also a technophile who continues to be amazed at the incredible opportunities and wondrous developments that the digital world has brought us. And that is something we should not forget here. Although this report has focused on the current surveillance economy and the many ways it disrespects what the UN has recognized as our right to privacy, we can envision a more positive future with an internet whose wonders can be fully enjoyed without concern that every breath we take and keystroke we make is being recorded in some distant server for whatever purpose the "owners" of our personal information eventually wish to put it.

Thanks again, and all the best for a healthy and happy 2021.