The Digital Privacy Dilemma

By Zaina K. and Amrita M.

Upon hearing of digital privacy violations, one often imagines the perpetrators to be huge, elusive entities. Visions of top-secret government departments and mega-corporations fill the mind. Yet it would be misguided to assume that these forces are the only dangers to accessing the online world. In these times, the average individual has at her fingertips the tools to trespass on the personal lives of others. The good news is that the average individual also has the tools to *protect* herself in the digital space.

Incidents of violating digital privacy (i.e. hacking) often attract much attention in the public sphere, likely because of the underlying sentiment of complete vulnerability created. Most are acutely aware of expert hackers who can apparently access even the most highly-protected data. Recently, headlines surfaced of an Adelaide teen who managed to hack into Apple's computer systems. This case is special as it does not just concern a single person; it concerns an innumerably long list of Apple users. The teen did not cause any financial loss for Apple, nor was customer information compromised at any point, so he was eventually released on a good behaviour bond. However, this incident illustrates how any one person has the tools at hand to potentially access the digital lives of others. A similar violation by another teen last year provides a scenario where the motives and actions were not as innocent. The teen hacked into Apple's systems and downloaded several sensitive files detailing how to infiltrate the tech giant's security. This could have very easily compromised the personal data of Apple's many users. Hence, such major incidents validate intense public fear regarding digital privacy, and highlight the need for better protective systems.

The question now falls on *what* exactly these hacking tools are. Although the methods used by the teens remain a mystery, there are other programs worth mentioning, programs which many online users can be susceptible to. Digital Information World lists several of these, such as "Facebook Autoliker 2019", which asks users for private account details under the pretense of providing lots of likes to particular posts. This program, however, uses the information to take control of the account. Thus, users should be wary of any program providing such services and should not give out account information to others. No trusted source should ask for such private details. There are also fake hacking tools which can instead hack the users, perhaps to enact some perverse sense of justice. One of these is called "Paypal Hacking Service 2019", which guarantees the transfer of money to a user's account at whim. However, the user is being tricked into giving up sensitive account details which can give complete access to the real hackers. Avoiding using hacking tools should keep one safe from such situations. In the end, all these tools rely on the user's actions for their effectiveness, and whether the user makes the choice to divulge her information online. If one is unsure about a website, Google provides an excellent Safe Browsing tool here to verify URLs. Another tip is to check for whether a website has HTTPS when inserting any sensitive financial data like credit card information. This features means that a user's online interactions with the website are encrypted to prevent someone from stealing her information. On Google Chrome the HTTPS feature will show up as "Secure" with a padlock next to it. Researching into the domain owner can also be useful. The many malware protection and system security-check tools on the market should not be ignored either.

In light of all the ways an individual's online information can be compromised, it would be natural to feel vulnerable to unknowable forces. There is comfort to be had, however, in new developments which focus on individual privacy. Forbes reports that by 2024, the identity verification industry will grow to $12.8 billion, from the current $6 billion. Furthermore, the new partnership between Mastercard and Samsung envisions more autonomy for users in regards to their online presence. Central to Mastercard's digital identity manifesto is the ability to choose what can be shared and in which way.
(*The manifesto is accessible here*)

Governments also have the power to fundamentally alter the field of digital privacy. Canadian companies are subject to severe repercussions if they violate the Digital Privacy Act, legislature that came into effect in November 2018. This Act is an amendment to the Personal Information Protection and Electronic Documents Act (PIPEDA), which states that organizations "must obtain an individual's consent when they collect, use or disclose that individual's personal information," according to the Office of the Privacy Commissioner of Canada. The Digital Privacy Act makes it mandatory for companies to record data breaches and inform the Privacy Commissioner and those affected. Failure to do so could result in fines up to $100 000 per violation. There is a valid argument to be made that this amount is insignificant for many of the larger corporations; however, PIPEDA does seem to place appropriate value on the privacy of Canadians. Bill C-51, the Anti-Terrorism Act, however, represents a significant regression in the field of digital privacy. The aim of this legislation is to identify security risks and prevent terrorist plots. The methods used include expanding the authority of government security agencies at the cost of citizens' digital privacy. Amendments have been made to restrict this authority and respond to people's concerns over the imposition on individual rights and freedoms, yet there is still some loss of online autonomy. This is seen as acceptable by both the Liberal and Conservative parties, implying that citizens themselves are ready to give up digital privacy to some extent for the cause of national security.

It is impossible to discuss the topic of digital privacy without addressing the topic of ethics. This is due to ethical dilemmas being at the crux of the difficulties in reaching concrete resolutions. All can ubiquitously agree on the need to draw boundaries where the individual's private life is concerned. Yet where exactly this line should be drawn is constantly under debate. Consider the following statements:

1) No one has the right to privacy
2) Everyone has the right to privacy

Between the first two statements, the better one is abundantly clear because the idea that everyone has the right to privacy is generally well-accepted. Now consider the following statements:

3) Everyone has the right to privacy as long as this right does not infringe on the rights of others
4) Everyone has the right to privacy even if this right infringes on the rights of others

At this point opinions begin to diverge; however, most individuals consider statement 3 to be the morally preferable choice: no one should have free reign to infringe upon the rights of others. Somewhat paradoxically, however, to agree wholeheartedly with statement 2 one must also accept statement 4: everyone has the right to privacy *regardless* of whether they are infringing upon the rights of others. The issues with statement 4 are clear; the authorities will not have clearance to trespass on an individual's digital privacy, even if this individual is under suspicion of a crime. In an age where many people share their most intimate details online, such a situation could severely impede police and government

investigations. Yet this also means that innocent individuals could be made incredibly vulnerable due to mere suspicion. This scenario highlights the downfalls of unfettered privacy, as well as the need to establish proper protocols to prevent arbitrary, or otherwise unwarranted, violations of digital privacy.

The flipside of the argument that everyone should have the right to privacy regardless of whether they violate the rights of others is the argument that national security should be prioritized ahead of an individual's right to personal privacy. This argument has gained support, particularly with the rise of terrorism. In a world where extremist groups make extensive use of the Internet to radicalize recruits, plan, and coordinate attacks on civilians, governments around the world have been attempting to maintain a balance between ensuring national security and preserving individual privacy rights. Unfortunately, finding the right balance between the two considerations is a significant challenge. For example, terrorist organizations such as ISIS made extensive use of both social media and highly sophisticated and encrypted methods of communication to coordinate plots such as the 2015 Paris attacks. However, with the restrictions on Western intelligence agencies regarding their ability to access private information, terrorist attacks become harder to prevent. This is supported by Nick Rasmussen, the head of the National Counter Terrorism Centre, who stated that the difficulty in tracking terrorists is "increasing over time." At its heart, the debate boils down to this question: Should an individual's right to personal privacy be given priority over the collective security of a nation?

It is important to keep in mind that users are not completely vulnerable to the dangers of the digital world. There are many tools out there to ensure user privacy, as there are many who support maintaining digital privacy. The ethical dilemma can get complicated when it comes to topics such as national security but still, a line must be drawn to protect one's private life. Voting for those who are familiar with this issue and understand the nuances between personal and collective security is necessary to finding satisfactory solutions. The best, and perhaps easiest, action that can be taken is to be more mindful and circumspect when using the digital space.

Sources:

Safe Browsing: malware and phishing – Google Transparency Report
Mastercard Introduces Consumer-Centric Model for Digital ID
Adelaide teenager gets good-behaviour bond for hacking Apple systems twice | Technology | The Guardian
Teen who hacked Apple told to use 'gifts for good rather than evil'
Teen Apple Hacker Avoids Jail in Australia After Serious Attacks - Bloomberg
The Digital Privacy Act: 5 FAQs About The New Mandatory Breach Response Obligations Effective November 1, 2018 - Privacy Protection - Canada
Personal Information Protection and Electronic Documents Act, SC 2000, c 5 | CanLII
PIPEDA in brief - Office of the Privacy Commissioner of Canada
Bill C-51 Could Be Used To Target Activists: Amnesty International | HuffPost Canada