Preface

Dangers of the Digital Age: Cyberthreats and Privacy

The Digital Age is the period in human history defined by the advent of personal computing and its integration into society. The era has also been called the Information Age, as one of the fundamental features of the era involves dramatic changes in the way that individuals create, manage, access, and share information. English statesman and scientist Sir Francis Bacon is credited with writing "scientia potentia est," which translates as "knowledge is power," and the substrate of the Internet is exactly that: data, the raw material that is used to create knowledge and thus power. While digital technology and the Web have empowered the populace with information, the Digital Age has also seen the rise of a new class of criminals and political agents who steal data from individuals, corporations, and governments, and use it for financial or political gain. The exploitation and misuse of personal data, both by criminals and by corporations and governments, also comprises a fundamental challenge to personal and intellectual privacy and has led to a global debate over the right to privacy and the ownership of data.

Ownership of Digital Data

If the Web is seen as a virtual community made up of individuals around the world participating in a massive global *agora* (in Greek, "a public open space"), then the individuals who participate can be seen as creating and presenting a virtual version of themselves through their communication and commercial transactions. In the 2010s, there is an emerging concept of digital citizenship, meaning the practices, standards, and norms needed to navigate the Web and participate in the digital economy. Digital citizenship is the principle that individuals who want to participate in the Web must learn how to use digital tools safely and responsibly and to behavior according to certain ethical rules that will prevent them from harming others with their digital activities.[1]

Properly defined, which consists of thousands of servers and hubs connected by more than 113,000 miles of cable, is the physical system that produces the Web[2] The Internet has been created through the combined effort of individuals, corporations, researchers, and government agencies. Internet Service Providers (ISPs), companies like Verizon and AT&T, create much of the infrastructure that makes the Internet and the Web work and then sell access to their infrastructure to individuals and other companies. The Web, by contrast, is made up of thousands of websites and services that individuals see when they use a computer or another digital device to access the Internet.

Data is the raw material of the Web and most data is created by digital citizens who use the Web for commerce and communication. The central question is: Who owns this data? The ISPs that transmit data over the Web claim partial ownership in return for access to their infrastructure. On top of this is another layer of companies, like Facebook, Google, and Amazon, who provide Web services. These companies also claim partial ownership of user data in return for their services, a fact that is stated in the corporate "terms of service" for companies like Facebook, Twitter, and Google. Companies collect and evaluate data from users and then use this data to market products and additional services to their customers/subscribers. In addition, because of laws established under the Patriot Act, the government has the right to collect and evaluate data transmitted through cellular or Web-based communication channels, which the government proposes is needed to help protect citizens from terrorism and other national security risks.[3] The digital citizens who provide most of the data traveling through the Internet therefore have the least control over what happens to that data because they only indirectly contribute to Internet infrastructure and cannot directly control the development of legislation that governs whether companies and government agencies are permitted to collect and use data voluntarily transmitted through corporate websites and digital equipment.

In the United States, there is no specific right to privacy explicitly guaranteed by the Constitution, though sections of the Constitution, such as First Amendment guarantee of free speech and Fourth Amendment protections against unreasonable government search and seizure can be used together to establish legal precedent for a general right to privacy in one's communications and beliefs. However, living in a society necessarily means surrendering some degree of privacy. Most Internet users may never feel personally affected by the fact that government agencies could potentially be reading their e-mails and text messages or that companies like Facebook and Google routinely monitor their Web-behavior in an effort to determine their likes and dislikes. Nevertheless, many are concerned about the erosion of privacy in the Digital Age and the US government and legal system has been slow to adopt measures to protect digital privacy.

Law Professor Julie E. Cohen argues that, at present, privacy is treated as an instrument used to protect other principles, like liberty or control of one's life, and that this view of privacy is part of the reason that governments and corporations have been able to ignore privacy concerns in favor of other goals such as protecting national security, preventing crime, or creating convenient new Web tools. Cohen proposes that the general concept of privacy should be redefined as fundamental freedom to engage in a process of self-development and to develop values that maybe distinct or separate from broader societal values and culture. In a 2013 article in the *Atlantic*, journalist Jathan Sadowski argued, "…we must decide if we really want to live in a society that treats every action as a data point to be analyzed and traded like currency."[4]

The Criminal Element

Another danger to digital privacy comes from cybercriminals who participate in an underground, illegal economy of data, stealing and selling information from digital citizens through hidden websites and servers comprising what is now called the Dark Web. Hackers have created a growing list of devious programs that help them steal data and wreak havoc on digital technology, including viruses, malware, adware, spyware, ransomware, and a host of other applications. A 2014 report indicated that cybercrime, including the theft of credit and debit card numbers, medical information, and personal data used to commit identity theft, costs the global economy more than $445 billion each year.[5]

Combating the criminal dangers of cyberspace requires digital citizens to stay on top of an ever- changing list of threats, and to learn about the behavioral changes and technological tools that can help keep their data safe and their Web-based communications private. There is also a continuing debate over the role of corporations in combating data theft. In numerous cases, cybercriminals have obtained consumer data by infiltrating the records of corporations like Target, Sony, and Home Depot, which collect and store e-mail addresses and credit/debit card numbers. Even with corporate data theft becoming more common, most corporations spend relatively little to prevent it because the costs of cybercrime are minimal compared to the costs of building better information technology (IT) security systems. For instance, when Home Depot was invaded by cybercriminals stealing 56 million credit and debit card numbers and 53 million e-mail addresses, the company lost $28 million, essentially amounting to less than 0.01 percent of the company's 2014 revenues.[6] This situation is fluid however, as consumer preference often dictates corporate policy. If consumers decide that cybersecurity is a priority and seek out companies that offer data-theft guarantees, corporations will likely adopt more aggressive security policies.

Politics in the Digital Realm

Cybercrime and cybersecurity aren't just a concern for consumers, but also for governments. The United States has been a leader in cyberwarfare, using hackers and digital tools to combat foreign threats, while the United States has also been the target of foreign cyberweapons. Increasingly, foreign governments have been linked to invasions of US corporations, stealing intellectual data that can be used to give other societies an economic advantage. With economic and political rivals like China, Russia, and North Korea working to develop cyberweapons and terrorist organizations like the Islamic State likewise using the Web and social media to spread their agendas, cyberwarfare is one of the biggest national security concerns of the twenty-first century.

In 2016, the United States was the victim of an entirely new type of cyberattack, when it was revealed that Russian hackers, operating under the direction of the Russian government, had stolen sensitive data from both the Republican and Democratic National Conventions and used the data they acquired to support Donald Trump's presidential campaign. While the revelation was shocking to many, and has

been criticized by Trump as an overt conspiracy to delegitimize his leadership, the National Security Agency (NSA), Central Intelligence Agency (CIA), and Federal Bureau of Investigation (FBI) have all verified that the hack occurred. Investigators aren't certain why the Russian government was willing to risk an international incident to help President Trump win the election, but Trump and allies' considerable economic ties to Russia and the fact that Trump, unlike past presidents, has not expressed any interest in pressuring Russia to improve its human rights record through sanctions, are believed to be aspects of why Russian President Vladimir Putin favored Trump as the next American president. There has also been speculation that Trump supporters and advisers such as Secretary of State Rex Tillerson, for instance, have close ties to the Russian oil industry.[7]

The Russian hack may be an example of the first known effort of a foreign government to use cyberwarfare to sway an American election and can be regarded as an act of political warfare directed against the United States. This event alone demonstrates the increasing importance of cyberwarfare and indicates some of the more subtle ways that political information can be weaponized.

No less dramatic in 2016-2017 has been the controversy over "fake news;" defined generally as any factually false news item created for profit or as propaganda to promote one's political/social views. Fake news is an old feature of US politics, but one with greater and greater influence as the share of digital citizens who get all or most of their news online has increased. The fake news environment of the 2016 election polarized the populace, obfuscating important issues in favor of sensationalized or patently false news items published through social media and unscrupulous websites. As thousands of Americans were deceived into believing that Hillary Clinton was involved in a child sex ring in Washington D.C., for instance, the legitimate media felt compelled to cover the controversy rather than focusing on more important issues, such as how Trump and Clinton, as candidates, were prepared to cope with income inequality, the decline of the US working class, racism, and inequality, or even, fittingly, national cybersecurity. The mainstream media spent so much of its time during the 2016 campaign fact checking outrageous claims by candidates and correcting rumors spread by fake news items that policy issues took a backseat for much of the year.

The perils of the Digital Age are numerous and complex, leaving many digital citizens confused about how to protect themselves from threats like surveillance, data theft, or the manipulation of fake news. Digital citizens are responsible for learning about cyberthreats and for taking the steps needed to mitigate the danger posed to themselves and others, but also must hold companies and their governments responsible for enacting legislation and policies to protect the digital privacy and intellectual property of their customers/constituents. When it comes to misinformation, the problem is more complex, but the solution is largely the same. Digital citizens cannot depend on politicians or media marketers to tell them where and how to get information, but must endeavor to develop a more informed critical approach to news and data, essentially becoming an *investigative news reader* to protect themselves from manipulation. If knowledge is power, then knowing where and

how to get reliable data about the world is the key that allows a person to transform that data into knowledge, and so into personal, economic, and political power.

Micah L. Issitt

Works Used

"Cyber Crime Costs Global Economy $445 Billion a Year: Report." *Reuters*, Reuters. Jun 9 2014. Web. 3 Mar 2017.

"Nine Elements." *Digital Citizenship,* Mike Ribble. 2017. Web. 3 Mar 2017.

Powers, Shawn M. and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago: University of Chicago Press, 2015.

Rubin, Jennifer. "Commentary: Why Did Russia Want Trump to Win?" *Chicago Tribune*, Tribune Media. Dec 12 2016. Web. 3 Mar 2017.

Sadowski, Jathan. "Why Does Privacy Matter? One Scholar's Answer." *The Atlantic*, Atlantic Monthly Group. Feb 26 2013. Web. 3 Mar 2017.

Sherman, Erik. "The Reason Companies Don't Fix Cybersecurity." *CBS News*, CBS. Mar 12 2015. Web. 3 Mar 2017.

Simonite, Tom. "First Detailed Public Map of U.S. Internet Backbone Could Make It Stronger." *MIT Technology Review*, MIT Press. Sep 15 2015. Web. 25 Feb 2017.

Notes

1. "Nine Elements," *Digital Citizenship*.
2. Simonite, "First Detailed Public Map of U.S. Internet Backbone Could Make It Stronger."
3. Powers and Jablonski, "The Real Cyber War," 150-65.
4. Sadowski, "Why Does Privacy Matter?"
5. "Cyber Crime Costs Global Economy $445 Billion a Year: Report," *Reuters*.
6. Sherman, "The Reason Companies Don't Fix Cybersecurity."
7. Rubin, "Commentary: Why Did Russia Want Trump to Win?"

1
Personal Cybersecurity

Credit: temniy

Digital lock sign on binaric background.

The Personal Data Dimension

Cybersecurity, or information technology security, is the effort to protect computers, networks, programs, and the data created and transmitted through these systems, from being intercepted, changed, or destroyed by others. Cybersecurity is an issue with personal, professional, and governmental implications and the very nature of the Internet, being a nebulously owned physical/virtual network involving millions of users, computers, corporations, and other entities, makes the process of protecting data both complex and *essential* for the evolution of society in the Digital Age. While the average computer user may feel he or she has little data worth protecting, every computer compromised by viruses, hackers, or other cyberthreats, is potentially a gateway through which the infection can spread.[1] A virus infecting a computer in suburban Iowa could potentially pose a threat to national networks or even federal government data.

In 2015, the cybersecurity industry, made up of companies providing software and other equipment to protect user and corporate data, was estimated to have a value of $75 billion, with expected growth to $170 billion by 2020.[2] Protecting data is not *only* a corporate concern that can be fixed with a technological bandage, however, as the effort to make the Internet safe is also a matter of public education and helping users to understand why protecting data is important and how behavioral and technological tools can help to protect them, and others, from cyberthreats.

The Illusion of Privacy

Who owns data? In the Digital Age, this is not a trivial or purely philosophical question. Data is the raw material used to create economic, social, and political power, and the ownership of digital data—even personal data—once it has been shared or transmitted through the vast nebula of the Internet, has NOT been determined.

Personal computing tools have made using the Internet *feel* like a private activity, but the sense of privacy is an illusion. Corporations routinely analyze and use data submitted by users to determine what kind of products a user might buy or to create pinpoint marketing campaigns. Governments have nearly unfettered access to private communications, including e-mails, text messages, social media posts, and even photos and audio picked up by built-in microphones and cameras, which they use at their discretion in the effort to identify threats to national security. The biggest risk to user privacy is the user her- or himself as ANY data shared through the Web, even privately between friends, can all too easily become public. News stories over the past decade document the increasingly common phenomenon in which individuals whose photos and posts have gone viral after unintentionally or intentionally being made public. In numerous widely publicized instances, Individuals have lost their jobs, been removed from office, or suffered public shame, ridicule, and

even threats to their safety. The fact that the phrase "Internet shaming," is now well known in the popular lexicon, reflects how often this occurs and how disastrous the consequences can be.[3]

Understanding Cyberthreats

Cyberthreats—defined as any individual, program, or entity with the potential to intercept, alter, or destroy data—come in many forms. Hackers are individuals skilled in programming or cybersecurity who are adept at entering secure computer systems or networks. The hackers known in the community as "black hats" who may also be called cybercriminals, penetrate security systems for personal gain, stealing personal information, credit card numbers, and a variety of other data that can be sold for profit.[4] One study described in a 2016 *Slate* magazine article found traced 320 different transactions involving cybercriminals selling data stolen from computer users, which resulted in between $1 and $2 million in profit. The criminals sold their stolen credit card numbers and other data through a series of clandestine websites known as the "Dark Web."[5]

Hackers have created a variety of tools to help them infiltrate computers and networks. Among the best known and most widely studied are viruses, which are programs that can replicate themselves (like their molecular namesakes) and can then spread from one computer on a network to others. Hackers can also use programs called "bots," that perform automatic functions once installed on a system, such as accessing or corrupting files or allowing a user in another area to gain access to a person's data, to watch them browse the Internet, to take complete control of their computer, or even to access built-in cameras and microphones to watch or listen to a computer owner.

In most cases, infiltrating a computer requires the computer owner or user to make some mistake that gives the hacker access. Cybercriminals may try to trick users to click on images or links or to visit certain websites by sending fake e-mails or instant messages. The message may appear to come from a friend or the criminal may try to entice the user with a financial reward or threaten the user by pretending to be from a known authority, such as the Internal Revenue Service (IRS) or the police. Once the user clicks on a link, message, or other active object, a program is installed on his or her computer. These programs, whether bots, malware, or viruses, cause the computer to perform various functions, such as sending out spam messages to individuals in the user's contact list, or giving the criminal who sent the bug access to the user's documents, photos, or other data. Hackers often use "phishing," which is a method of data theft that uses deceptive messages, links, websites, or other means to trick users into volunteering sensitive information, such as their social security number, account numbers, or other data typically used in security questions such as the person's grade school friends, first pets, mother's maiden name, etc.

Personal Cybersecurity Tools

For those who think the risk to their data is minimal, visiting the website www.haveibeenpwned.com can be illuminating. The website provides a list of e-mail addresses found in various "data dumps," which are collections of data publically posted after cybercriminals hacked into companies like Yahoo!, Target, Google, and LinkedIn. Many of the largest, most widely used companies have been hacked, and the data provided by users to these sites has therefore been compromised as well.

So, how does one protect his or her personal data? The process involves both behavioral changes and technological tools. A short guide to some of the basic steps might be as follows:

Behavioral:

1) Use caution when posting on social media and communicating on the Web. Consider that all social media or Web-based communications could become public.

2) Do not open e-mails or messages from unknown senders or that appear unusual.

3) Clean up one's social media presence.

Technological:

1) Use stronger passwords, at least 10-characters, but preferably 30-characters.

2) Use a password manager.

3) Do not use the same password on multiple sites/programs.

4) Use two-factor or multifactor authentication when available.

5) Use a Tor Browser to keep Web activity private.

6) Use a Virtual Private Network (VPN) to enhance privacy on the Web.

To start with, Internet users should NOT consider the Web a safe place to share sensitive or potentially damaging information and this is *especially* true for social media. Users should think critically about *what* they share online and *how* information is being shared. Posting on social media is essentially like speaking aloud in a crowded room, surrounded by mixed company. The message may be meant for friends, but can easily be overheard by the strangers on all sides. Most of those strangers probably don't care, but some might, and they might share that information with others.

It is important for Web users to understand that their cyberidentity, the information and personality that they present to other social media users and companies through their presence on the Web, shopping habits, and other virtual activities, is

the same as crafting a public persona. Others are watching, so every user must be aware and take steps to ensure that he or she is presenting a version of themselves fit for the public. In addition, experts recommend cleaning up one's social media presence regularly, going through sites and networks to remove data that might be compromising.[6]

In terms of technological tools, there are many choices for personal cybersecurity. Antivirus and antimalware software can help to protect personal computers from malicious programs, while other tools help protect a user's privacy when browsing the Web or help to keep their personal data secure when visiting their favorite sites or Web services.

Password strength is a major area of concern for Web security, as it takes only minutes for a hacker using sophisticated programs to hack into a system protected by a typical 8-character password. Longer passwords, with combinations of letters, numbers, and special characters, are typically recommended. It is also important NOT to use a password that could be easily guessed by someone with knowledge of the individual's family, life, or history. Security specialists recommend using 10-character passwords for sites or programs that contain little sensitive data, and 30-character passwords for especially sensitive sites or programs such as banks, medical insurance sites, etc.

Alternatively, users are increasingly choosing to use password managers, which are software systems that generate complicated passwords for all the sites and programs that a user accesses and only require the user to remember a single password, which is used to access the password manager program.[7] In some cases, users may have the option of using multifactor authentication systems, which are security programs that require the user to provide more than one method of authenticating their identity before they can gain access. For instance, 2-factor authentication (2FA), used on many secure sites, typically requires the user to first enter their password and user name, and then complete a second step, such as using a fingerprint or voice print to authenticate their identification.[8]

More advanced tools may be of interest to those who are more concerned about Web privacy. For instance, VPN- service, which creates a secure, encrypted connection between the Web and the user's computer, essentially scrambles a computer's unique identification address, thus making it difficult to gain information about the user's identity and location. Virtual private network services do not protect against all forms of data intrusion, but are sufficient to protect user data against most casual data leaks, including the processes used by companies for corporate data mining and some levels of digital surveillance.[9] Another step for those concerned about Web privacy is to use a Tor browser when browsing the Web. TOR was developed by researchers looking to create a browser that was more difficult to hack and resistant to surveillance and shifts data back and forth between multiple points, making it more difficult for any individual intercepting data to determine where the data came from or where it is ultimately going.

The Internet is a fantastic tool that has ushered in a new era in information and collaboration that continues to shape the world in myriad ways, but the public

consciousness has not caught up with the technological revolution. Data is power and power needs to be handled with respect, protected from foreign and domestic threats, and made safe from accidental damage or distribution. Personal cybersecurity *is* public security and, in some ways, is *also* national security and learning about the behavioral and technological tools needed to keep data safe can be considered, in the changing postdigital revolution world, akin to learning new rules of citizenship.

Micah L. Issitt

Works Used

Eddy, Max. "The Best VPN Services of 2017." *PC Mag,* Ziff Davis, LLC. Jan 31, 2017.

Gordon, Whitson. "Here's Everywhere You Should Enable Two-Factor Authentication Right Now." *Lifehacker*, Gizmodo Media Group. Dec 10, 2013.

Holt, Thomas. "Here's How Hackers Make Millions Selling Your Stolen Passwords." *Slate*. Slate Group. Jun 29, 2016.

Magid, Larry. "Why Cyber Security Matters to Everyone." *Forbes*. Forbes Inc. Oct 1, 2014.

Morgan, Steve. "Cybersecurity Market Reaches $75 Billion in 2015; Expected to Reach $170 Billion by 2020." *Forbes*. Forbes, Inc. Dec 20, 2015.

Pogue, David. "The Bright Side of Internet Shaming." *Scientific American*. Oct 1 2016. Web. 25 Feb 2017.

Rubenking, Neil J. "The Best Password Managers of 2017." *PC Mag*, Ziff Davis LLC. Feb 15 2017. Web. 26 Feb 2017.

Sammons, John and Michael Cross. *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy*. New York: Syngress, 2017.

Wang, Jie and Zachary A. Kissel. *Introduction to Network Security: Theory and Practice*. Hoboken, NJ: Wiley Press, 2015.

Zimmerman, Carlota. "6 Ways to Spring Clean Your Social Media Presence." *The Huffington Post,* Huffington Post Co. Apr 8 2015. Web. 25 Feb 2017.

Notes

1. Magid, "Why Cyber Security Matters to Everyone."
2. Morgan, "Cybersecurity Market Reaches $75 Billion in 2015."
3. Pogue, "The Bright Side of Internet Shaming."
4. Wang and Kissel, *Introduction to Network Security*, 25-30.
5. Holt, "Here's How Hackers Make Millions Selling Your Stolen Passwords."
6. Zimmerman, "6 Ways to Spring Clean Your Social Media Presence."
7. Rubenking, "The Best Password Managers of 2017."
8. Gordon, "Here's Everywhere You Should Enable Two Factor Authentication Right Now."
9. Eddy, "The Best VPN Services of 2017."