Emerging Writers

Volume 2 Article 2

5-2019

Big Brother, erm Data is Watching and We Don’t Seem to Care.

Gary Hopkins

Gary Hopkins

First-Place Winner

Academic Category

2019 Emerging Writers Contest

Big Brother, erm Data is Watching and We Don't Seem to Care.

"Woke up, fell out of bed, dragged a comb across my head. Found my way downstairs and drank a cup and looking up I noticed I was late…" John Lennon's words from the classic Beatles song, "A Day in the Life," (Lennon and McCartney) describe the simple beginning to a typical day back in 1967.

Let's compare that to today. Your sleep-tracker app digitally nudges your smartphone's alarm and beep-beeps you awake. You turn on the television to the morning news and check the weather app, Facebook, Instagram, or your other social media sites. You tell Alexa to put on a favorite tune as your smart home controller lights the way downstairs and dials in a comfy setting on the thermostat. You smell your breakfast blend brewing as your Wi-Fi coffee maker percolates that perfect first cup. You're ready to start your day. This scene is quite a contrast from 1967, and much trickier to put to music.

Perhaps the most significant difference, however, some fifty years later, is that the devices that make up your morning routine may be spying on you and collecting your data without your knowledge or consent. We're no longer in the innocent time of that quirky Beatles tune and instead have slipped into the cautionary realm of the Police's, "Every Breath You Take," (Sting) wherein, as the lyrics go, "…every move you make, I'll be watching you." We're now in the era of "Big Data," and honestly, it's a leviathan.

To illustrate just how gargantuan Big Data has become, our combined output of data globally is approximately 2.5 quintillion bytes a day (Schultz). As of 2017, the United States alone produces roughly 2.7 million gigabytes of internet data per minute. That is 8.3 megabytes of data per minute for every man, woman, and child. Each of us streams out data morning, noon and night. Much of it is our most private information. Our phone calls, text messages, internet activities, online shopping, entertainment viewing habits, GPS location, social security numbers, job history, medical records, credit, banking, financial information, and much more, are collected and warehoused in massive data centers throughout the world (Marr). As researchers Esma Aïmeur and Manual Lafond pointed out in their paper, "The Scourge Of Internet Personal Data Collection," from our birth to our death, the bits and bytes that make up our digital life are aggregated and analyzed outside of our homes–and mostly outside of our control (Aïmeur and Lafond).

At the same alarming rate that our data is amassing, the efficiency with which corporations and the government exploit it for profit is accelerating (Martin). What then has become of our right to privacy? Some analysts believe we may have already passed the point of no return for privacy rights in this country. The thinking is that data collection has become so interwoven into the fabric of our economy that limiting its gathering is now virtually impossible. "You can't put the toothpaste back in the tube," as the saying goes.

Equally alarming is the growing erosion of our rights as citizens in the United States. A right to privacy is a fundamental aspect of being an American, guaranteed by the 4th Amendment to the Constitution. However, in the digital age, and the era of Big Data, we have become complacent when it comes to our liberties. We seem to willingly and eagerly trade them for each new online functionality, a so-called "price of convenience," as described by corporations that deal in the digital trade (Ketelaar and van Balen). In this age of Big Data and eroding privacy, it is vital

that a new, multi-faceted approach to online privacy and data collection be instituted to protect us quite literally from ourselves.

Before starting this essay, I hadn't ever considered how much of my private information I had willingly provided on countless websites or through my smartphone or car. When technology entered my life in the 1980s, it was all about the promise of convenience and a better life. There was little to portend how insidious and interwoven into our lives all technology would become. We are dependent on our digitally connected devices, and in some cases, we are addicted to them. Instead of alleviating our worries, they have brought on an entirely new set of concerns. Who has our information and for what purpose are they using it?

I began using personal computers in 1986, relatively close to their first introduction. I started on the then-groundbreaking Apple IIe. I was in advertising, an industry that relied heavily upon innovation and information, so the benefits of desktop computing became quickly apparent. I was using computers heavily in business and at home throughout the late 1980s and early 1990s and was there as the "world wide web" became a reality.

As the internet increased in size and interconnectivity, so did my reliance on it. I looked for ways in which my clients could benefit from the power of this "connected world." At that time, the protections for personal information online were in their infancy. Congress had only established the first cyber-security laws to protect people from online fraud and abuse in 1986.

By 1993, the pioneering browser, Mosaic, had been created and allowed users to "surf" the world wide web more easily, albeit at the then blazing speed of 14.4 kbps. As accessibility grew, so did the opportunities that capitalized on these connected users and the internet took its first steps into online commerce. I could place orders for goods through the internet and not bother with the hassles of phone calls or "snail" mail. The security of my credit card information barely crossed

my mind as I rushed to shop in the new cyber world.

My experience is not unlike the thousands of early adopters of the internet. My data has been in digital form and "out there" for almost three decades. Fortunately, I haven't experienced identity fraud but not because I've been cautious. I plunged into internet use with abandon. I've filled out countless online forms without really knowing the full measures of the website's security. I have recklessly traded my data for functionality from an app, or a website. In short, I am somewhat of a worst-case scenario for online data collection. I hadn't considered how much of my right to privacy I was giving away. Nor did I realize to what lengths marketers were willing to go to harvest and exploit my information. As the internet has grown to the current behemoth of interconnected devices, the so-called, "internet of things," so has the threat to both our data and our right to privacy.

What does that privacy threat look like in my household? My family has two desktop computers, three laptops, three smartphones, three tablets, two Apple TV devices, a broadband cable TV box and Wi-Fi hub, a wireless printer, and two cars that both have onboard infotainment systems. All of these devices are connected to the internet and providing vast amounts of data on myself and my family members. The worst offenders are the smartphones, in our case, iPhones. They are with us continually, always on, always watching, listening, and tracking us.

Through embedded orientation and gyroscopic sensors and GPS, our smartphones track our whereabouts as we scurry about town on errands or sit in gridlock on Interstate 85 (Caddy). Social media apps and websites keep us connected to family members and friends with well-wishes, celebrations, anniversaries, and photos of our intimate moments. We text, email, post, and tweet all manner of news about ourselves. According to tech blogger Jeff Schultz of the Micro Focus Blog, as of 2017, there were 3.8 billion internet users worldwide (Schultz). At work, many of us can

quite literally perform our entire job online, without ever printing a single piece of paper.

I recently started working at a digital marketing firm and have a desk with no file drawers. I print out only a few documents, keeping them stacked neatly on my desk, but can see a point where I probably won't even do that. We keep all of the company work files in the Cloud. My workspace has moved into the ether. At this point in history, unless you're entirely off the grid, each of us has a fully-realized digital persona, with definable traits, attributes, and behaviors. That "digital self" is as much a part of me as my flesh and blood.

Moreover, it's this digital presence, our online fingerprints, and footfalls, that researchers, data analysts, and marketers covet so much. Our online information is the currency of the digital age. It's as valuable as it is vulnerable. But is our concern over our data privacy enough to make us change our behavior? Do we care enough to change?

A 2013 study by the Pew Research Center after the Edward Snowden leaks (Rainie), shows that for the most part, people believe they conduct themselves online in a manner that protects their most private data from hackers and criminals but less-so from companies, the government, and law enforcement. The study also reveals that an overwhelming majority of people (91 percent) believe that consumers have lost control over what data is collected by companies and how they use it. Very few of us think our online information will remain private and secure. However, our responses to the perceived threat of an online privacy breach are varied. In many instances, our degree of concern is inversely proportional to our level of comfort and familiarity with technology.

Research by Annika Bergström, Ph.D., of the University of Gothenburg in Sweden confirms this theory. Her line of inquiry covers specific areas in which online privacy may be of concern for people and measures their reactions to them. The study involves a relatively large and diverse set of respondents. It measures their responses from "very concerned" to "not an issue for

me," relating to typical online activities including conducting searches, communicating via email, social media interactions, and debit card transactions. The study revealed that the more we use the internet and other digital technologies that collect our data, the less we seem to be concerned about our privacy (Bergström)–which leads us to a paradox.

A ground-breaking research paper by Susan Barnes entitled, "A privacy paradox: Social networking in the United States," (Barnes) sounded an alarm over personal privacy concerns in the context of social media and introduced the "privacy paradox," more than a decade ago. The privacy paradox represents the dissonance between the beliefs of varying groups of online social media users and their behaviors. In essence, it is the willingness with which some users freely share information online followed by their subsequent dismay that their openness can have unintended and harmful consequences. This research goes to the heart of whether we genuinely care about our privacy. We know the behavior is risky, yet we engage in it seemingly regardless of the potential consequences. So, do we actually care about our privacy?

To try and understand the phenomenon further, I conducted an informal, 10-question survey among the many people I connect with through Kennesaw State University, Facebook, and LinkedIn. I made it clear in the survey invitation that the responses would be anonymous and that I would not collect IP data. I didn't want to contribute to the privacy issue myself! The 1,751 people I invited to participate were from all ages and socio-demographic backgrounds. I received forty-seven responses–an approximate three percent response rate which is relatively typical. The respondents' ages were forty-seven percent 18-34, thirty percent 35-54, and twenty-three percent 55 years or older. Seventy-seven percent were college educated.

The participants in my survey behave as I do. Despite their education and experience, most found online privacy agreements hard to understand and for the most part do not read them. Only

thirty-four percent believed online companies took their privacy seriously and only five percent thought their online data was well-protected. Despite the apparent concerns of my survey participants, eighty-five percent shop online at least once a month, unequivocal confirmation of the privacy paradox. We seem to be unable to help ourselves. We care about our privacy, but at this point, technology is too much a part of how we conduct our daily lives to change how we behave.

My informal study mirrors the findings of a study conducted by Jonathan Obar, Ph.D., and Anne Oelderf-Hirsch, Ph.D. In their paper entitled, "The Biggest Lie On The Internet: Ignoring The Privacy Policies and Terms Of Service Policies Of Social Networking Service," (Obar and Oelderf-Hirsch), seventy-four percent of respondents skipped privacy policy information. Those that did read the policy spent only an average of seventy-three seconds reading it.

What can we do to protect our right to privacy? Left to their own devices, the purveyors of Big Data have been in a veritable wild west, filled with lawlessness and recklessness. Author Ieuan Jolly, recognized internationally as a leader in the areas of data and technology, provides an excellent overview of the laws and regulations concerning individual online privacy protection and data collection. His easy-to-read primer reveals that right now, a patchwork of federal regulations and state laws govern data collection and online privacy. There seems to be no cohesive, top-down strategy by which our privacy is protected (Jolly). As a result, it appears that government agencies and the states divide jurisdiction and enforcement of online privacy laws. This overlapping, jurisdictional responsibility is particularly relevant in the face of the massive consumer data breach that transpired at Equifax last year as well as the Facebook user data breach this year.

The tools we have are either too complicated or not robust enough. Car companies are currently only governed by an informal agreement among themselves to not share a driver's location, health, or behavior to third parties (Krisher and Durbin). It's an excellent idea but can

easily be circumvented without the weight of the law behind it. A field study conducted by a group of researchers at the School of Computer Science at Carnegie Mellon University found that the privacy permission management on smartphone apps is overly complicated and not intuitive. Pretty much the opposite of "smart." Their work reveals that smartphone users would benefit greatly from easily-implemented "privacy nudging," which would automatically alert users to apps that put their privacy at risk (Almuhimedi et al.).

Further study of the work by Esma Aïmeur and Manuel Lafond exposes that the entire discipline of privacy enhancing technologies, or PETs as they are known, may be ineffectual. Their research describes the inherent pitfalls of PETs including "re-identification," a term describing the assembling of pieces of available online data to uncover a person's identity. In this manner, your private data can be pieced together like a puzzle by an algorithm and not have to come directly from you. The conclusion reached in their paper is that there may nothing we can do individually to protect ourselves online (Aïmeur and Lafond). Despite this bleak outlook and the seeming end to our right to privacy, I for one believe that we can fix this and I'm not alone.

There is a growing demand for government and private enterprise to do more to protect our privacy. During the time I have been researching and writing this essay, privacy concerns seem to have reached a boiling point. The most recent news that Facebook allowed personal data to be collected by a third party without the knowledge or consent of its users appears to have been the final straw. Mark Zuckerberg, Facebook's founder, has been in the nation's capital, testifying before Congress as to the safety of our private information online. In reality, there have been seventeen significant data breaches dating back to 2006, the worst of which was Yahoo's astounding revelation that three billion user accounts had been compromised (Armerding). Hackers made off with user email addresses, passwords, real names, dates of birth, and telephone numbers

of Yahoo users in the most massive data breach in history. Our collective outrage at the lack of protection for our private information online is long overdue.

Amazingly, there are still voices out there, even within our government that believe there are enough laws on the books to protect our privacy. They think enforcement is the key. If the "cost-of-doing-business" slap on the wrist that Equifax may receive for compromising the credit histories of 143 million users, including dates of birth and social security numbers, is an example of enforcement, then we absolutely must do better (Henning).

An early and prescient work on privacy in the face of technology by Robert Laufer and Maxine Wolfe from 1977, contains this rather ominous quote, "Technological changes can have unintended consequences for our understanding of what constitutes privacy or for perceived privacy options." Their work warned of the dangers of a society where full-disclosure may be the norm. We are coming dangerously close to that reality. What does the future hold for our right to privacy? I imagine quite an Orwellian existence, where the most substantial loss is individual liberty. A fantastic and frightening world such as that revealed in the movie Minority Report, based on the short story by Philp K. Dick, where outdoor advertising assaults you with profoundly personal information as you walk down the street (Minority Report).

The implications of online data collection and privacy protection go to the very heart of our nation. Privacy is an integral part of freedom–so much so that we have protected it in our Constitution. Does the current state of data collection violate our privacy and therefore our rights? Should, "Terms of Service Agreements," and "Privacy Policies," for websites, devices, and software applications be more explicit and transparent by law? They are, after all, a contract. Should we give up our 4th Amendment rights merely by clicking a button on some app?

As the "internet of things" continues along its blistering exponential growth trajectory, our

fundamental right to privacy is eroding at the same alarming rate. Despite the evidence of this growing threat, we are trapped in inaction and without any truly effective means by which to protect ourselves. Therefore, it has become vital that a new, multi-faceted approach to protecting our online privacy be instituted. While I'm not proposing an in-depth examination of all possible solutions, I believe several steps are essential. The first must be to extend the protections of the 4th Amendment to the Constitution by including our online activities in the definition of our homes. The second would be to pass federal laws to require uniform, transparent, and unambiguous privacy agreements as well as rigorous prosecution of violators. We must educate the general public on the risks to their private data and provide instruction on how to protect it. We can follow in the footsteps of the European Union and enact sweeping privacy protection legislation such as the General Data Protection Regulation (GDPR) going into effect May 25th of this year.

We are the generations that created the digital information age. We are responsible for the explosive growth of connected devices and the pervasive and invasive internet of things. It is up to us to clear up these privacy concerns now. Even though the data is already out of hand and the genie may be out of the bottle, we can, and we must act. We must overcome the privacy paradox and become our own best advocates when it comes to our personal information online! We can solve this issue for future generations and perhaps ultimately come to a more mutually agreeable relationship with Big Brother, erm Data.

Works Cited

Aïmeur, Esma, and Manuel Lafond. "2013 Eighth International Conference on Availability, Reliability and Security (ARES)." *IEEE Computer Society*, pp. 821–828, ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6657326&isnumber=6657192.

Almuhimedi, Hazim, et al. "Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging." *SCS TECHNICAL REPORT COLLECTION*, School of Computer Science Carnegie Mellon University, Dec. 2014, reports-archive.adm.cs.cmu.edu/anon/isr2014/CMU-ISR-14-116.pdf.

Armerding, Taylor. "The 17 Biggest Data Breaches of the 21st Century." *CSO Online*, CSO, 26 Jan. 2018, www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

Barnes, Susan B.. "A privacy paradox: Social networking in the United States." *First Monday* [Online], 11.9 (2006): n. pag. Web. 5 Mar. 2018. http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312#author.

Bergström, Annika. "Full Length Article: Online Privacy Concerns: A Broad Approach to Understanding the Concerns of Different Groups for Different Uses." *Computers in Human Behavior*, vol. 53, 01 Dec. 2015, pp. 419-426. EBSCO*host*, doi:10.1016/j.chb.2015.07.025.

Caddy, Becca. "Here's How Your Phone Is Tracking You Right Now." *TechRadar*, TechRadar The Source for Tech Buying Advice, 9 Apr. 2016, www.techradar.com/news/phone-and-communications/mobile-phones/sensory-overload-how-your-smartphone-is-becoming-part-of-you-1210244.

Henning, Peter J. "Hack Will Lead to Little, If Any, Punishment for Equifax." *The New York*

Times, The New York Times, 20 Sept. 2017, www.nytimes.com/2017/09/20/business/equifax-hack-penalties.html.

Jolly, Ieuan. "Data Protection in the United States: Overview. A Q&A guide to data protection in the United States." *Thomson Reuters Practical Law*, Loeb & Loeb, 1 July 2017, content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=%28sc.Default%29&transitionType=Default.

Ketelaar, Paul E., and Mark Van Balen. "The Smartphone as Your Follower: The Role of Smartphone Literacy in the Relation between Privacy Concerns, Attitude and Behaviour towards Phone-Embedded Tracking." *Computers in Human Behavior*, vol. 78, Jan. 2018, pp. 174–182., ac.els-cdn.com/S0747563217305605/1-s2.0-S0747563217305605-main.pdf?_tid=3a305f5b-d9e5-4201-a0a4-2407b572130d&acdnat=1520362228_5a8c01fba3bda23e2a0571f520727e2a.

Krisher, Tom, and Dee-Ann Durbin. "Q&A: The Data Your Car Collects and Who Can Use It." *AP News*, Associated Press, 29 Sept. 2016, apnews.com/31c018cdbc634d42a7c97d04774954b1.

Laufer, Robert S.1 and Maxine2 Wolfe. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." *Journal of Social Issues*, vol. 33, no. 3, Summer1977, pp. 22-42. EBSCO*host*, proxy.kennesaw.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eue&AN=16370005&site=eds-live&scope=site.

Lennon, John, and McCartney, Paul, The Beatles. "A Day in the Life." *Sgt. Pepper's Lonely Hearts Club Band*, EMI Studios, and Regent Sound Studio, London, England, 26 May 1967.

Marr, Bernard. "Big Data: 20 Mind-Boggling Facts Everyone Must Read." *Forbes*, Forbes Magazine, 19 Nov. 2015, www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#123fab3017b1.

Martin, Kirsten. "Data Aggregators, Consumer Data, and Responsibility Online: Who Is Tracking Consumers Online and Should They Stop?." *Information Society*, vol. 32, no. 1, Jan-Feb 2016, pp. 51-63. EBSCO*host*, doi:10.1080/01972243.2015.1107166.

Minority Report. Directed by Steven Spielberg, Production by Amblin Entertainment, Cruise/Wagner Productions, and Blue Tulip Productions, Distributed by 20th Century Fox and DreamWorks Pictures, 19, June 2002.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *TPRC 44:* The 44th Research Conference on Communication, Information and Internet Policy 2016, 26 August 2016, papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465.

Rainie, Lee. "The State of Privacy in Post-Snowden America." *FACTANK News In The Numbers*, Pew Research Center, 21 Sept. 2016, www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

Schultz, Jeff. "Micro Focus Blog." *How Much Data Is Created on the Internet Each Day? Micro Focus Blog*, Micro Focus, 10 Oct. 2017, blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/.

Sting, The Police. "Every Breath You Take." B-Side Single of *Murder by Numbers*, A&M Records, London, England, 20 May 1983.