ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Facebook Poses a Massive Risk to National Security

But It's Worse than You Think…

April 2018

Authored by:

James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

ICIT Analysis: Facebook Poses a Massive Risk to National Security

But It's Worse than You Think…

April 2018

Authored by: James Scott, Sr. Fellow, ICIT

Center for SPACE WARFARE STUDIES

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Center for Cyber-Influence Operations Studies CCIOS

Support ICIT

Through objective research, publications and educational initiatives, the Institute for Critical Infrastructure Technology, a 501(c)(3) cybersecurity think tank located in Washington, D.C., is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark. Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

http://icitech.org/support-icit/

Upcoming Event

Contents

Was Anyone Surprised?

The Facebook-Cambridge Analytica scandal was not shocking or unprecedented. The sensitive behavioral and PII data of over 87 million users was collected and exchanged without knowledge or consent and was leveraged in massive political influence operations. Meanwhile, the information of over 2.2 billion Facebook users was vulnerable to open-source intelligence (OSINT) tools capable of scraping personal details from the platform. “Web scraping” is the digital process of automatically loading and reading the pages of a website for later analysis. It amounts to machine automated web browsing. Companies often deploy automated web browsing products to gather data necessary to track performance ranking of products, monitor social media, conduct customer support, track competitors’ pricing and inventory, or aggregate information to optimize supply chain operations. Scraping is also used to monitor sites for fraud, perform due diligence checks on their customers and suppliers, and to collect market data [1]. Online threat actors could aggregate and sell the data, tailor attack campaigns, precision target specific individuals, or otherwise, employ the information in dozens of other nefarious schemes.

Facebook's inability to secure user data or protect their privacy is not surprising because dragnet surveillance capitalists turned dragnet surveillance propagandists remain under-controlled to the point that they knowingly operate on a spectrum from criminally negligent to negligently criminal. These firms redefined the Internet and online activity, and in many ways, they conceived and continued to dictate the laws and regulations governing their operation. The rise and prosperity of "data capitalists" is the symptom of a pervasive cybersecurity and privacy epidemic that permeates the industry and culture of America. While it is essential that negligent data brokers face the consequences for their nefarious activities, it is also vital that the underlying disease that founded the environment of their growth be addressed with a shift in cultural cyber-hygiene, meaningful legislation, and disruptive innovation.

At an April 10, 2018 joint hearing of the Senate Commerce and Judiciary Committees, Senator John Kennedy commented to Facebook CEO Mark Zuckerberg, “You can go back home, spend $10 million on lobbyists and fight us, or you can go back home and help us solve this problem.” For each minute that Zuckerberg sat before the Senate and House committees, Facebook’s stock regained so much value that Zuckerberg’s net worth rose $3 billion, or about $10 million per minute. Without significant support, it does not appear likely that legislation can remediate the privacy harms inflicted on consumers by Facebook and other tech giants. Instead of asking “What legislative solutions can prevent another Cambridge Analytica?” or “How can Facebook be regulated?” legislators and key decision makers can better serve the public by assessing “What consumer privacy protections are deficient or missing?” and “What incentives can be implemented to increase competition and innovation in stagnant tech markets that are dominated by dragnet surveillance capitalists, while ensuring greater security and privacy

safeguards for users?" Without sweeping changes, judicious forethought, and comprehensive understanding, the short-term solutions of today may facilitate the problems of tomorrow [2].

We were Distracted by "Free Services" while Privacy Rights Diminished

The issues at the heart of the Facebook-Cambridge Analytica scandal are also at the heart of much of the surveillance-based, advertising-powered popular web. Sweeping data collection, manipulative advertising, and indiscriminate and unscrupulous information exchanges now define the majority of online interactions [3].

Social media users deserve the right to leave platforms with which they are not satisfied, without fear of how captured data from their experience could negatively impact their future online and offline interactions. Users should have the right to leave and to delete their information and the entire account. Users who decide to leave a platform, such as Facebook, should be able to easily, efficiently, and intuitively eliminate their account and freely take their uploaded information away and move it to a different one in a usable format. To online dragnet capitalists, data is the product gained from users and resold to third-parties. If an exchange is unfavorable to the user, they should be able to "take their business elsewhere." "Data portability" or "data liberation" is fundamental to user control over their information and is essential for the promotion of competition in the free market. Data liberation depends on informed consent and user control. Companies must be prevented from exploiting data portability by misleading users or from obfuscating the collection, retention, and exchange of user data. The removal of data from platform servers and affiliates' servers should be comprehensive and permanent. It should not amount to just disabled access or single source removal. If a party captures data as part of an agreement with the user and shares that information with third-parties, the company should be responsible for ensuring that the user data is removed from all third-party systems [3].

Deleting social media is not an attractive choice for many of Facebook, Twitter, etc. billions of users. For some, societal and other factors may entirely diminish the viability of a choice. For many, social media platforms are their only way to connect with friends, family, and organizations. Some businesses rely on the digital vectors to garner larger audiences and fulfill their customers' needs. Numerous communities and interest groups hosted on digital platforms are not available in many users' cities and areas. Facebook, Twitter, and other social media mega-corporations lack viable general alternatives.

Privacy harm is a unique form of injury with specific boundaries and characteristics. Violations of privacy, in the strict legal sense, do not need to occur for an individual to suffer privacy harm. Privacy harms often happen when the autonomy or equality of a person is at stake due to the capture or weaponization of their information. Privacy harm can be either subjective (the

unwanted perception of observation) or objective (the unanticipated or coerced use of information concerning a person against that person). Subjective privacy harm describes unwelcome mental states – anxiety, embarrassment, fear – that stem from the belief that one is being watched or monitored. Government surveillance and information collection by a third-party are examples of subjective privacy harms. Objective privacy harms are adverse, external actions justified by reference to personal information. Examples include identity theft, the leaking of classified information that reveals jeopardizes an individual or national security, or the targeted use of information in coercive efforts to alter the behavior of a data subject. The subjective and objective categories of privacy harm are distinct but related. The categories represent, respectively, the anticipation and consequence of a loss of control over personal information. A simplified interpretation is that objective privacy harm occurs after the occurrence of subjective privacy harm, typically when the data is leveraged against the subject; however, the two harms can also arise as distinct harms [4].

For most, the negative switching costs resultant from the loss of access to massive user bases and associated network effects far outweigh the benefits of leaving the platform to combat potential privacy harms because users have been systematically programmed to devalue their information and privacy. When incidents occur, too many Americans immediately respond, “no one would want my data because it is not valuable enough” or some derivative statement. A cybersecurity, cyber-hygiene and privacy awareness renaissance is necessary to dispel the apathy that empowers the negligent actions of dragnet surveillance capitalists turned propagandists.

Domestic and International consumers face a complex dilemma in their decision of how to engage with social media in the future because “ignore the platforms” or “delete your accounts” may no longer be reasonable or possible options. Most will choose to accept the risk and harm, and many will intentionally shy away from understanding the issue at all. Dragnet surveillance capitalists know how users are positioned because they dictated the terms of their dependence, the conditions of their usage, and the obstacles to their escape [3].

Lawmakers and regulators need to consider codifying users’ right to informed decision making, right to control one’s information, right to notice, and right to redress. Responsible social media companies should ensure these rights and be held accountable for failures to protect users from privacy harms. Facebook, Twitter, Google, and others must respect user privacy by default and by design. Users are the source of the revenue and popularity of these “too big to fail” platforms; users should not have to forfeit all their privacy rights just to engage in the services that capitalize on their existence [3].

Privacy Exchanges Depend on Behavioral Economics

The most fundamental economic transaction is that of *exchange*: two individuals engage in a trade. For example, one person, ``the seller'' gives another person, ``the buyer'', an apple; in exchange, the buyer gives the seller some money [5]. In the case of modern social media, users give companies their information in exchange for access and utilization of communication platforms that are otherwise unavailable. The transaction is made in "good faith" with the expectation that the user will not lie about their details and the company will not abuse the data; however, as social media platforms have become more ubiquitous and pervasive, the public has become proportionally less aware or informed about the conditions of the unspoken transaction. Meanwhile, Facebook and similar platforms have increased the amount of data they collect and implemented mechanisms to ensure that the user cannot choose what data is collected, how the data is used or shared, or whether the information is accurate. The compounding of mechanisms such as background mobile application privileges or the necessity of a verifiable email address or mobile number force users to divulge more and more accurate information which dragnet surveillance capitalists can market at increased rates to third-parties that remain unknown to the user. In effect, over the past decades' users devolved from partners in a mutually beneficial transaction into captive product generators who are kept dependent on social media platforms via peer pressure, neurochemical dependencies, and other amoral control schemas.

Evaluating the value of data or privacy are malleable and mutable because valuations differ based on who is asked, and how the question is presented. According to Dr. Alessandro Acquisiti, individuals face privacy trade-offs of two types: transactions in which individuals are offered tangible or intangible benefits in exchange for their personal information, and transactions in which individuals are provided protection of their personal information, but at some tangible or intangible costs. The categories often get conflated in policy and empirical debates about the value of privacy. The availability of an alternative option (i.e., paying for privacy or having protections) empirically impacted privacy valuations of data subjects. Those presented with the opportunity to give up privacy assurances for a material benefit made decisions that suggested much greater concern for privacy than those who could, in effect, purchase greater privacy at a price. One interpretation of the findings is that when privacy is a limited commodity, as it is when users cannot regain it and have little or no control over it, users place greater emphasis on the value of their information and what few decisions they have concerning its use. Endowment effects powerfully influence individual privacy valuations. Individuals give away their personal information for minuscule rewards, such as a discount card, when they perceive limited risk. However, when confronted with how that data could be leveraged to influence their behavior or how it could be weaponized against them if stolen, users become much less likely to share their information willingly. The difference between the

observed behavioral patterns results from an informed choice, control of one's data, and the option to provide consent. Social media companies and other data brokers dissuade consumers from seeking information or vying for control or consent options through the strategic delivery of dopamine and through faux-control mechanisms, such as privacy policies, that provide the illusion of notice and choice.

Empires are Built on a Molecule

Facebook is an empire of empires, built upon a dopamine molecule. Research from Dr. Nenad Sestan and Dr. André Sousa of the Yale School of Medicine and others has shown that dopamine levels are one of the key differentiators between human beings and other apes. Dopamine, as one of the major neurotransmitters, carries many different kinds of message, only some of which are known and understood. Its core function is in learning the extent to which a reward differs from expectations. It is also vital for movement control and plays a role in memory, attention, mood, cognition, and sleep. Sestan and Sousa found that 1.5% of the neurons in the human striatum produce dopamine, three times more than in the ape striatum. They hypothesize that the cells could contribute to human-specific aspects of cognition or behavior. Biologically, dopamine galvanizes humans to take actions to meet their needs and desires by anticipating how they will feel after the activity is complete.

When the Cambridge Analytica scandal became public, many organizations and individual users demonstrated their disapproval of the negligent actions of Facebook and Cambridge Analytica by deleting their accounts. Facebook CEO Mark Zuckerberg claims that the viral "#DeleteFacebook" movement had little meaningful impact on the platform. In March, at the advent of the revelation of the scandal, Facebook lost around $60 billion in market capitalization due to a 5 percent drop in shares. At the same time, Google searches for "How to delete Facebook" spiked, and some companies pulled advertisements from the platform [6]. Sean Parker, the founding president of Facebook (retired 2005), recently stated that the social network was founded not to unite us, but to distract us. "The thought process was: 'How do we consume as much of your time and conscious attention as possible?'" he said at a November 2017 event. Parker continued that Facebook's architects exploited a "vulnerability in human psychology." Whenever someone likes or comments on a post or photograph, he said, "we… give you a little dopamine hit". Tech companies lace their products with mental 'hijacking techniques' because they understand what causes dopamine surges in the brain. They lure users into creating and sustaining "compulsion loops" [7].

Social media sites emulate the makers of slot machines by distributing irregularly timed rewards. Surveillance capitalists essentially engineer their platforms to be addictive, engaging, and encompassing. Dopamine is released when a gambler feels "lucky" [7]. Casinos make

money by maintaining gamblers' attention through strategic bursts of "luck." Similarly, Facebook, Twitter, Google and other platforms reward user behavior with targeted microbursts of dopamine. Their profits depend on the number of unique users, their market share, the average linger time of users, and the pervasiveness and ubiquity of the platform. Each of those factors contributes to the quantity and quality of data that can be aggregated and either sold or algorithmically weaponized. Facebook and Twitter want users to have the instinctual, primal urge to check their feeds and statuses, even when working or interacting offline. Google is algorithmically "optimized" to reward users with fast and relevant results as a mechanism of sustaining a dedicated and dependent user base; consider, how much less information is memorized because "it can be Googled" or how many fewer drivers now utilize maps, directions, or even GPS units because Google Maps and other travel services are almost always immediately available. Every application and platform that is "free" generates revenue through targeted ads and data curation. Users are programmed to overlook their caution through strategically triggered dopamine deliveries.

The methodology is based on the work of American psychologist BF Skinner, who found that the strongest way to reinforce a learned behavior in rats is to reward it on a random schedule. Constant rewards would increase dependency in the short-term but may dull reception in the long-term. As a result, the rate at which users receive ads, messages, or updates (via GPS, Alexa, etc.) are studied, monitored, and controlled [7].

Though the premise might seem flimsy, consider that any application can be built according to this model that exchanges dopamine for data, and nearly every successful app employs the premise to one degree or another. As a demonstration of the success of this methodology, consider that Facebook redefined the Internet landscape by persuading users to compulsively check the site for enticing social affirmation cues. The capabilities and limitations for so-called "persuasive technology" to influence behavior are only just becoming understood, but the power of the dopamine system to alter habits is already known to drug addicts and smokers. Every habit-forming drug, from amphetamines to cocaine, from nicotine to alcohol, affects the dopamine system by dispersing many times more dopamine than usual. The use of these drugs overruns the neural pathways connecting the reward circuit to the prefrontal cortex, which helps people to tame impulses. The more an addict uses a drug, the harder it becomes to stop. Addiction occurs when the brain is repeatedly overstimulated from unfiltered and unnaturally large dopamine deliveries that result from addictive and algorithmically optimized rewards systems. Over time, subjects lose their willpower as their brain chemistry is altered by abuses of artificial triggers. The capacity for dopamine to facilitate the formation of addictive behavior can be seen in studies of some Parkinson's drugs, which, in flooding the brain with dopamine, have been shown to turn close to 10% of patients into gambling addicts. For dragnet surveillance capitalists, the longer the user is engaged, the more data can be harvested, and the

more ads can be delivered. For the emerging propagandists, which are the next evolutionary stage, the dwell time of users is proportional to the levels of indoctrination and propagation of their disinformation and other materials [7].

The concept of behavioral economics that we can change the behavior of others by putting them into particular situations instead of through coercion or chemical induction is still being studied. Training people via systems to release dopamine for specific actions could cause conditions where people cannot escape the system of their own volition. While the methodology can be used to entice positive behaviors, it can also be leveraged for systemic data mining, pervasive platform dependence, and sustained influence operations.

Manipulative Policies Remain Capricious and Impenetrable

To have a contract, you have to have several components. Binding agreements consist of a (1) offer; (2) acceptance; (3) consideration; (4) mutuality of obligation; (5) competency and capacity; and, in particular circumstances, (6) a written instrument. With Facebook and other dragnet capitalists it is worth questioning whether sufficient explicitly outlined and defined terms are offered in the terms of services to waive one's right to personal privacy (Offer) or whether the terms were written in such a way that the user could have reasonably understood or expected that their information would be collected and used in this way, or that such a possibility existed (acceptance). Even if the user gave permission to Facebook for the collection and use of personal information, on a case-by-case basis, did the user provide sufficient permissions to Facebook to exchange their information with third party entities, or did the user give Facebook direct permission to use the information as Facebook pleased with third-party entities (acceptance). Does the contract established in the terms of service constitute a meeting of the minds of the parties, as well as whether the terms of the contract were conscionable, balanced, or fair, and made of the parties own free will (consideration). Free will is essential to agreeing to and understanding the terms (consideration; competency and capacity). A written agreement does exist, but is the agreement readily accessible to the user after the initial presentation or can it be changed at the whims of the service provider with only cursory notification to the user?

Terms-of-Service are an Antiquated "Defense" from a Simpler Internet

Privacy policies and terms of service agreements continue to be the hallmark of dragnet capitalists' power and legal defense despite offering an overwhelmingly asymmetrical advantage to service providers while affording them the capability to circumvent informed consent and notice and choice in all but the most literal interpretations of the word of law. The relinquishment of privacy rights and recourse options are buried within layers of legal jargon

and wordplay that is intentionally designed to sap reader attention and dissuade active engagement. It is the digital equivalent of negotiation via an attention-based blockade.

Cases involving the enforceability of terms of service are decided on a case by case basis. In most instances, the courts tend to hold the contract as valid; an intentional and deliberate deception typically must be shown on the part of the contractor in order to nullify it. Meanwhile, contracts made through manipulation and force are not enforceable. Usually, usage of social media is seen as an act of free will and acceptance of a "take-it-or-leave-the-platform" offer. Given dragnet capitalists dependency-based model, should the legal rigidity of terms of service agreements continue to be seen as resolute?

Further consideration may be given to the micro-transactions of privacy between Internet users and digital platforms. Does one waive a right to privacy merely by having a page or having public information on that page? Should clicking the “like” button on an unaffiliated page relinquish privacy rights to Facebook? Why does Facebook need to retain ownership of images posted on the platform; should it retain rights to users’ images even if they are only bystanders in a photo uploaded on someone else’s page?

Online Legal Policies are Intentionally Misleading and Vague

Privacy policies were created by web merchants and online data curators allegedly to assuage consumers’ fears of data mismanagement; however, privacy policies fail to build trust between consumers and merchants because their content, language, and presentation are poorly designed. Privacy policies are actively written and employed predominantly to protect companies from lawsuits based on privacy legislation, rather than address user concerns of data misuse. In the majority of instances, they force consumers to surrender their rights under “take it or leave it” style terms of usage. Users do not read privacy policies because the language is too complicated, too vague, and too deceptive [8]. The information would be more comprehensive and more digestible if terms were described in plain language and the information was presented in a table or a use/data matrix but such mechanisms do not favor digital brokers and does not feature comprehensive legal jargon sufficient to holistically release the site from liability and responsibility for privacy and security harms incurred by the users as a result of the negligent practices of online operators.

According to a 2007 study by Dr. Aleecia McDonald and Dr. Lorrie Cranor, it would take the average American 81-293 hours just to skim the privacy policies of the unique websites they visit annually. This averaged to about 40 minutes per day which was immense compared to the 2007 estimate that consumers used the Internet for 72 minutes per day. For an estimated workforce of 221 million, that amounts to an average of 54 billion hours/ year. They estimated that the average user would lose approximately $3000 per year ($2474 work; $530 home) in

opportunity costs to skim privacy policies. This would nationally average to 675.5 billion in opportunity costs per year just to skim each visited site's privacy policy once. Costs for reading were much higher. Costs for actually comprehending the policies were not determined [10]. Consider that the study reflected Internet usage and wage costs from 2007 when the Internet was still budding, Facebook was still a start-up, and some users still depended on dial-up Internet. It is estimated that every day in 2017, the average adult spent 235 minutes on their mobile device Internet and 235 minutes on PCs, laptops, or tablets [9]. Daily Internet usage is over 6.6 times the 2007 values; though much of that time is committed to engaging with addictive platforms like Facebook, so conversion of privacy policy opportunity costs may not translate. Nevertheless, consider that each second on those platforms and sites generates data that is monitored, aggregated, exchanged, and leveraged in online advertising, product development analytics, and other methodologies.

Users Remain Unaware of Collected, Stored, and Weaponized Data

The Cambridge Analytica incident was not a data breach. It was precisely how Facebook's infrastructure was designed to work. Facebook has allowed third parties to violate user privacy on an unprecedented scale, and, while legislators and regulators vie to understand the implications and put limits in place, users are left with the responsibility to make sure their profiles are properly configured. The scale of the violation of user privacy reflects how Facebook's terms of service and API were structured at the time.

Leaving Facebook is not an option for many users who either depend on the platform for businesses and connections or are addicted to the dopamine surges delivered via interaction with the platform. Users that want to prevent their data from being processed through Facebook's API can restrict their privacy settings; though doing so will disable all platform apps (like Farmville, Twitter, or Instagram) and will prevent logins from external sites that rely on the Facebook login. The loss of interconnectivity and the convolution of settings menus are some of the primary disincentives leveraged to dissuade user response to the violation of their privacy rights.

Following the Cambridge Analytica incident, users were made aware of the ability to assess what information Facebook has collected and stored. Other than evaluating their account and activity logs, users can go to **Settings** and click "**Download a copy of your Facebook data**." Users can restrict some of the data that Facebook collects, stores, and shares. Log into Facebook and visit the App Settings page (or go there manually via the Settings Menu > Apps). From there, click the "**Edit**" button under "**Apps, Websites and Plugins**." Click "**Disable Platform**." Another setting can be altered to restrict data leakage if disabling platform entirely not desired. By default, other people who can see your info can bring it with them when they

use apps, and your info becomes available to those apps. The setting limits the personal information accessible by apps that others use. You can limit this by following the directions provided, clicking "**Edit**" under "**Apps Others Use**" and then unchecking the types of information that you don't want others' apps to be able to access. Similar procedures exist for Google, Twitter, and other platforms [11].

Online, "Free" Indicates an Exchange of Privacy or a Forfeiture of Data

Behavioral Advertising relies on digital trackers (cookies, super-cookies, etc.), first-third party information transactions, and aggregated information profiles. A great deal of the information transferred is non-personal (allegedly anonymized) information, such as session cookies, browsing history, system specifications, etc. If a user logs into an account during their session or accesses unique information, then the tracker information can be associated with that user and used for targeted behavioral advertising (de-anonymization). In some countries, notably the United States, IP address does not count as PII and it can also be used to target ads. Further, some first parties, such as Amazon and other retailers, collect user information such as purchase history and they either use the information to target ads or they sell the information (and membership information) to data brokers who aggregate user profiles and sell them to advertisers who target ads. Social media networks aggregate user interests, associations, and user posted personal information (age, area, school, birthday, religion, political views, etc.). In short, the personal information that can be collected for digital and "physical" behavioral advertising include: name, age, gender, income range, address, phone number, purchase history, interests, browsing habits, memberships, friends and family (through social networks), and other ad specific personal information to ascertain users' behavior and interests in digital and physical realms.

Facebook claims that its "product is social media – the ability to connect with the people that matter to you, wherever they are in the world. It's the same with a free search engine, website or newspaper. The core product is reading the news or finding information – and the ads exist to fund that experience." Facebook does offer users a "free" social media platform designed for interconnectivity and digital media consumption. However, it remains a publically traded, for-profit company whose profits are dependent on the quantity and engagement of its users. Despite their consternation, the insights garnered from the algorithmic weaponization of user data and the time that users spend interacting on the platform remain their actual product. Advertisers pay to deliver tailored messages to Facebook users. Consequently, Facebook's assertion that they do not consider users to be products is only semantically accurate. Facebook considers users to be product generators in the same fashion that a dairy farmer requires cows to generate milk.

In a blog post, Facebook promised that it does not sell sensitive PII data to advertisers or third-parties, claiming, "So our promise is this: we do not tell advertisers who you are or sell your information to anyone. That has always been true. We think relevant advertising and privacy aren't in conflict, and we're committed to doing both well." Their admission is only a half-truth. Facebook delivers focused ads to specific users. Facebook's defense is that consumers are protected by undue influence because Facebook stands as an intermediary in the influence operation. The post continues,

> "As people use Facebook, they share information and content – whether it's liking a post, sharing a photo or updating their profile. We use this information to give you a better service. For example, we can show you photos from your closest friends at the top of your News Feed, or show you articles about issues that matter most to you, or suggest groups that you might want to join. Data also helps us show you better and more relevant ads. And it lets advertisers reach the right people, including millions of small businesses and non-profits who rely on Facebook every day to reach people that might be interested in their product or cause. Data lets a local coffee shop survive and grow amid larger competitors by showing ads to customers in its area. And it lets a non-profit promote a diabetes fundraiser to those interested in the cause."

Facebook obfuscates its unnecessary dragnet surveillance and negligent data-exchange practices through the illusion that it acts on behalf of the consumer. It attempts to hide that it aggregates and leverages the immense data sets as a strategic dragnet capitalist strategy whose sole purpose is maximized revenue at minimal costs. Revenue is proportional to the quantity and quality of captured information and insights. Meanwhile, the cost is inversely proportional to privacy and security safeguards. Even though users are at least inadvertent product-generators for Facebook's machine, if not products themselves, Facebook does not want that incite evangelized. Facebook is not alone.

Thousands of Other Data Brokers Lurk in the Digital Background

Facebook collects data from posts, likes, photos, things typed and deleted without posting, behavioral activity while not on Facebook and even offline activity. It buys data from others, and it can infer sexual orientation, political beliefs, relationship status, drug use, and other personality traits without the need for personality test like what Cambridge Analytica developed. Thousands of other companies continue to lurk in the shadows of the Internet as Facebook stands "apologizing" in the limelight, setting a precedent and normalization standard for the desensitization of the populace and the ineffectual response to everyday abuses perpetrated by negligent data brokers [12].

There are at least 2,500 to 4,000 data brokers in the United States whose sole business depends on buying and selling consumer PII. Last year, a breach at Equifax dominated the news cycle after hackers stole the personal information of around 145.5 million Americans, nearly half the population. The information included Social Security numbers, birth dates, addresses, and driver's license numbers [12]. The data was collected and aggregated without consumer consent and in many cases, without their knowledge. Nevertheless, after an incident that exposed the data of nearly half the country, Equifax suffered less than minimal consequences by arguing that "incompetence is not illegal" and due to postponed action by the Consumer Finance Protection Bureau [4] [13].

Companies like Facebook and Google offer free services in exchange for personal data. Google's surveillance does not dominate the news, in part because it has a level of control over the news cycle, but the platform may know more about users than they know themselves. Consider, no one lies to a search engine. It captures and stores users' interests and curiosities, hopes and fears, desires and sexual proclivities. Most Android devices come pre-installed with at least one Google application, if not the entire suite, which perpetually catalogs every transmitted byte. Websites visited are tracked by Google through its advertising network. Gmail accounts monitor correspondence and word selections. Movements are tracked via Google Maps and background location services [12].

Every layer of modern life is actively monitored by one or dozens of shadow data brokers. Mobile devices are ever present and continuously monitored for location history (home, work, hobbies, and other addresses), interests (cookies, order that sites are visited, dwell time, daily schedule, etc.), proximity to other devices, etc. Dragnet surveillance capitalism drives the internet because lawmakers, regulators, and everyday users never took action to prevent the rise of the shadow economy [12].

Most “free” services and many paid ones participate in personalized advertising, psychological manipulation, political influence operations, or other activities that feed into and depend upon the continued suppression of consumers’ privacy and security rights. In comparison, Cambridge Analytica was unsophisticated and ineffectual. In his UK testimony, Dr. Aleksandr Kogan said that he believed that the findings of the company had little to no discernable impact because Facebook already had the data and influence necessary to alter geopolitical and socio-economic communities. Cambridge Analytica did not provide any insights or data that were not previously known and weaponized by social media dragnet surveillance propagandists. If the actual extent of surveillance capitalism came to light, there would be broad demands for limits and regulation. However, most of the public remains intentionally unaware of widespread predatory surveillance, and they are incentivized and conditioned to stay that way [12].

Beware the Illusion of Reform and "Self-Regulation"

In the wake of Cambridge Analytica, many tech firms, including Facebook, Twitter, and Google, are feigning "proactive" responses. In reality, the alterations to terms-of-service and flimsy privacy safeguards are actually in anticipation of the May 25, 2018, General Data Protection Regulation (GDPR) deadline. Among other things, GDPR mandates are that personal data of EU citizens can only be collected and saved for "specific, explicit, and legitimate purposes," and only with the explicit consent of the user. Consent can't be buried in the terms and conditions, nor can it be assumed unless the user opts-in [12].

The GDPR will offer consumers in the EU more control over their data and outlines requirements for data collection, storage, and use. It will also impose potentially steep fines on companies with poor data-handling practices and those that experience data breaches in which they are found at fault.

Since most surveillance capitalists collect data internationally, they are forced to adapt to mitigate full exposure of their amoral operations. GDPR is composed of 99 articles and 173 recitals that are used to help interpret the law. Sanctions for noncompliance can be a fine up to €20 million (approximately $24.6 million) or up to 4% of the annual worldwide turnover (net sales generated by a business) of the preceding financial year, whichever is greater. GDPR affects any business that operates in the EU and foreign companies that process the data of EU citizens. In our global economy, this is virtually every business. Furthermore, a business must flow these requirements down to all their vendors [14]. GDPR forces a measure of transparency. It is not comprehensive, but after decades of ignoring predatory data collection and weaponization, affording consumers some protection is better than continued inactivity. GDPR addresses who has data, whether it is accurate, what is being done with it, who are likely third-parties, how information is secured, and whether details can be deleted [12].

While the regulations are limited to the personal data of consumers living in the EU, they apply to any company handling, transmitting, or storing that data, whether it has a physical location in the EU or not. Marketing technology (martech) companies that process data for and receive personal data from their customers are included even though they don't collect personally identifiable information per se. Consumers are assigned a cookie with some random, unique value to tie specific website events together. With the GDPR, the notion of personal data is extended to include online identifiers such as IP addresses and cookie values. These identifiers do not identify an individual, but if you combine these with additional information, you can identify a person. Under GDPR, securing data often depends on pseudonymization, based on where the data was processed so that it cannot be attributed to a specific person. Hashing and encryption are examples of pseudonymization. Companies will have to either obtain consent or have a legitimate interest to process PII. They will be required to comply with requirements

such as data portability, also referred to as the "right to forget." The right to forget revolves around the concept that consumers have a right to demand the deletion of their data from companies that have that data, even if they previously have permitted its collection. Firms are exploring pseudonymization mechanisms, such as database normalization, to circumvent the impact of the right to be forgotten. In effect, the user data will be deleted, but the derivative insights will remain provided they do not directly identify the subject. On the other hand, GDPR may inspire a "privacy-by-design" approach to system construction and acquisition [15].

Surveillance Capitalism Risk National Security and Consumer Safety

From influence operations to targeted attacks against niche personnel, governments and businesses around the world are concerned about the risks posed by social media, which is playing an increasingly important role in both national and enterprise security. Borders between people, once based on geography, are now based on online platforms. Facebook has over 2 billion users, YouTube has 1.5 billion, WhatsApp has 1.2 billion, WeChat has 938,000. Social media is an unavoidable and unfettered facet of daily life. As more platforms become stages for public demonstrations and news distribution or evolve into pulpits for world leaders and other prolific figures, Twitter, Facebook, and similar platforms will become both more influential and more fertile for attacks. Social media is the ideal arena for information operations and false account because social media provides the perfect amount of anonymity and distance for attackers to launch comprehensive virtual campaigns, from afar, with a minimal dedication of resources. Accounts and activity are easy to fake. For instance, a fake Twitter account for the US Central Command reached over 110,000 followers. Soon, fraudulent and spoofed accounts will be the biggest threats to the businesses since attackers can easily and simultaneously target employees and customers. The potential impact of these attacks further expands the power and influence social media companies hold over consumers and businesses. The actions or inactions of Facebook, Twitter, or Google can potentially shift the economy or devastate a competitor.

Data privacy is vital to national security because individuals are often the targets of the first layer of attack campaigns. In a 10,000-person study conducted by Harris Poll and sponsored by IBM, researchers found 78% of US respondents say an organization's ability to keep their data private is "extremely important" but only 20% "completely trust" them to do so. Without significant change, the risk posed by dragnet surveillance propagandists cannot be mitigated. Consider that Facebook continues to collect data even when users aren't on the platform. Several websites and apps use Facebook services, like its login and analytics tools, to personalize their content. When users visit a site or app that uses its services, Facebook gets info even when the user is logged out - or doesn't have a Facebook account at all [16].

In addition to targeted influence operations and induced behavioral control, dragnet aggregate information poses a significant risk to average consumers and niche critical infrastructure personnel if stolen by a malicious adversary. Below is an unsophisticated attack chain following an incident [17].

Create a Repository of the Stolen Data

Hackers inventory the stolen data and identify victim's authentication credentials, personal information such as names, addresses, and phone numbers, as well as financial information such as credit card details. Much of this information can be leveraged for future attacks or sold off for capital to finance other attacks [17].

Sell the Personal Information

Attackers package and sell personal information such as names, addresses, phone numbers, and email addresses. They are typically sold repeatedly and in bulk to maximize profit. The more recent the records are, the more valuable they are on Deep Web markets and forums [17].

Target Data is the Most Valuable

Once the baseline personal information is accounted for, hackers identify lucrative accounts via authentication credentials. Government and military addresses credentials, company email addresses, and passwords for large corporations are typical priorities. Weak account credentials and reused credentials are leveraged against additional targets. On occasion, PII is used to steal additional accounts that may be connected to a compromised email, etc. [17].

Sell Credit Card Information

Financial information such as credit card numbers are typically packaged and sold in bundles of tens or hundreds. A “broker” sometimes buys the card information, then sells them to a "carder," who goes through a series of phony purchases to avoid detection. The "carders" first uses a stolen credit card to buy gift cards. TThe gift cards are used to purchase physical items. The carder may sell the items through legitimate channels like eBay, or through an underground website on the dark web. According to McAfee, a credit card with a CVV2 code on the back is worth between $5 and $8, but if it also has the bank’s ID number, it could go for $15 online. If the stolen information has the victim’s complete information, that could go for up to $30 [17].

Residual Stolen Data is Offloaded in Bulk

After several months, remaining authentication credentials are bundled and sold in bulk at a discounted price on open dark web markets. At this point, most of the credentials are worthless since the company has most likely discovered the breach and taken steps to fix it [17].

File Phony Tax Returns to Receive Refunds

Fraudsters will take stolen identities and file fake tax returns to receive tax rebates from both state government treasuries and the IRS. In most cases, data sets are collected piecemeal from social media, OSINT tools, and the stolen data. Though the IRS reports that total fraud losses dropped 14% last year, fraudsters still stole $783 million in 2016 [17].

Open Fake Medical Practice and File Fraudulent Claims

The federal government estimates that roughly 10% of the money spent on the program is lost to fraud and waste. Trustwave reported this year that one medical record from a single individual fetches $250 on Deep Web. Criminals set up fraudulent medical practices and submit false claims based on stolen information. They also prey on the elderly or most any other citizen by sending bills for small amounts that people assume they need to pay. Incremental payments quickly accumulate and do not take much effort on behalf of the attacker [17].

Steal Intellectual Property

Companies spend millions of dollars annually on research and development. The United States Trade Representative recently reported that IP theft by the Chinese alone costs US businesses at least $50 billion annually. Most of these hacks are sophisticated actions sanctioned by nation-states or are the efforts of insider threats. Other hackers also sell stolen data, such as emails, piecemeal, which can be used in layered attacks [17].

Leverage the Information is a Multi-Level Influence Operation

Firms like Cambridge Analytica have publicly bragged about their alleged ability to influence the values and thoughts of citizens. Real sophisticated attackers can outsource or easily launch cheap social media-driven influence operations by utilizing machine learning and artificial intelligence systems against stolen data and the public data collectible from OSINT tools. The derived insights are used to develop weaponized memes that are tested and then deployed across multiple vectors while the adversary seizes control of the overarching narrative.

Users Deserve Common-Sense Online Privacy Rights

As Grindr, LinkedIn, Under Armor, and hundreds of other companies can attest, Facebook is hardly alone in its recent failure to protect user data. The crucial difference is that Facebook is massive in comparison to most companies and its failure managed to capture the attention of the public and key-decision makers [2].

Right to Informed Decision-Making

Companies that aggregate and disseminate data should be prepared to disclose to users what information Is collected, how it is employed, and with which third-parties it is shared. Users deserve a clear and intuitive interface that divulges the platform's practices and that enables

users to make informed decisions concerning their data, how it is used, and whether or with what organizations it is shared [2].

Right to Control

Data usage should be "opt-in" by default instead of "opt-out." Currently, when users engage with digital platforms, they do not retain control over their data or disclosure of their information, even when the specific data can be used to identify or target them. Predatory companies can collect and share user data without explicit authorization. These organizations resort to deception because the functionalities they offer in exchange for user data are not equivalent to the value of the data that users provide [2].

A codified Right to Control restores ownership of data to its subject rather than continuing to allow dragnet organizations or predatory firms to retain legal ownership of whatever data they collect or purchase. The right would require services to obtain explicit permission before making secondary use of data, making any changes that could share new data about users, that could share users' data with new parties, or that would use data in new ways [2].

Right to Leave

The #DeleteFacebook movement epitomizes some users' drive to leave platforms and services that fail to meet their needs, secure their data, or protect their privacy. At the time of this writing, users lack the inherent right to delete their entire data set or account from all service and affiliate servers. In reality, if a customer does not like a restaurant they are free to choose another. If a buyer does not like a seller, they can seek another, and vice-versa. In the digital space, switching costs and a severe disparity in "data portability" or "data liberation" inhibit meaningful competition and deny subjects control or ownership of their information even if they sever their relationship with the service [2].

Right to Notice

Though brief delays may be necessary to ensure continuity, mitigation, or remediation, when incidents occur that result in the unauthorized access or disclosure of sensitive information, Facebook and other online data custodians must notify subjects as soon as possible [2].

Right of Redress

Rights mean nothing if there are no mechanisms of enforcement or recourse. Meaningful legal redress includes elimination of terms-of-service provisions, which are used to asymmetrically protect the service instead of the user, and it necessitates the adoption of clear, public, and unambiguous terms and commitments that define lawful operation of service providers and if breached, subject social media platforms to unfair advertising, competition, or other actionable legal claims [2].

Right to Data Confidentiality

Whether a user's information is shared with third-parties or specific third-parties, should be left to the data subject. Insights derivative of the data may still be leveraged, and advertisements can still be delivered based on the terms of the platform.

Right to Data Availability

As data subjects, users need access to collected data to audit the accuracy of the information or to make informed decisions.

Right to Data Integrity

If data is inaccurate, users should be permitted to correct the information so that they are subject to the inaccurate insights or potentially embarrassing or dangerous circumstances.

Right to Security

Collected data should be secured according to its value and its potential impact on the data subject if inadvertently disclosed or accessed. Data custodians should be liable for breaches and other incidents that inflict immediate or potential privacy or other harms on consumers.

Right to be Forgotten

Subjects deserve the right to remove their information from a platform as a mechanism of protest, portability, security, or for any other reason. Ownership of data should revert to subjects when the formal or informal exchange with the platform ends.

Consumer Privacy Rights Must be Restored and Safeguarded

Companies cannot be trusted to provide users with these fundamental rights, and they cannot continue to self-regulate or "hold themselves accountable" because every incident jeopardizes the well-being of millions of users and increasingly risks national security. False advertising laws, consumer protection regulations, and unfair competition rules have been implemented; however, so far they have not been enough to incentivize significant behavioral remediation in negligent data aggregators and brokers. A fine of a few million dollars is not a penalty when data is amorally or unlawfully exchanged for tens of millions. Under the current rules and regulations, negligent data brokers and dragnet surveillance capitalists can account for the risk of an incident being discovered as "a cost of doing business" if their illicit activities are ever discovered. For many companies, such as Facebook, civil action or widespread social disincentives do not pose a significant deterrent to adverse behavior because users are treated like products and many avenues of redress are forbidden by the terms-of-service which was intestinally designed to deter users from reading or understanding its conditions before engaging with the platform [2].

Courts often dismiss data breach lawsuits due to a narrow definition of “harm” that results from the equation of consequence to immediate financial impact. The problem with this approach is that not all harms are fiscal and that most exploitations of user data that result in financial loss do not occur immediately after an incident. Actionable laws are implemented to protect individuals from premeditated crimes like assault or murder, to protect against acts that cause mass fear, or to safeguard the public from the future and contingent harms of corporate pollution, or medical malpractice; yet, meaningful laws have not been enacted to provide protections or legal recourse for individuals’ whose data is disclosed, accessed, or exchanged without their explicit permission [2]. Federal and state legislatures have the capability to codify:

- Greater incentives for companies to secure user data according to its value or impact potential
- Limits on permitted access and collection of information
- Strict data retention restrictions
- A prohibition on terms-of-service waivers that force users to forfeit legal rights and recourse options
- Steeper penalties and other disincentives for organizations that fail to secure sensitive data

Mechanisms need to be implemented to discourage companies from pursuing surveillance-based business models. At the very least, those who combat mass consumer surveillance should be afforded as much legal protection as corporations. For instance, under the current laws and regulations Facebook can legally harvest the personal data of every person who visits a webpage featuring a "like" button; however, authors of browser plugins that block the button may face technical and legal barriers. Third-parties are effectively inhibited from offering users protection or control over how Facebook and other social media companies collect data. Removing some of the barriers created through broad interpretations of the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, and contractual prohibitions on interoperability, could increase privacy, innovation, and competition in the digital realm [2].

Platforms should be required to issue and declare clear and meaningful standards of portability that provide users the ability to leave the platform with their data at their discretion. Robust data portability would lower switching costs and empower users; as a result, innovators, startups, and small businesses would not have to combat tech giants. Further, social media titans would be under more significant pressure to meet user needs and innovate to stay competitive. These standards may be difficult to legislate because codification could impede long-term flexibility, adaptability, and protection. Incentivization may prove more effective at inducing lasting behavioral shifts. Nevertheless, even short-term incentives for data custodians

to innovate and secure user data and privacy could spur a shift in an otherwise stagnant sector [2].

Consumers should not be forced to believe Facebook, Google, ISPs, or others' concerning how data is gathered, stored, exchanged, retained, or used. Nor should consumers be beholden to the negligently lackadaisical security and cyber-hygiene practices of organizations whose continued operation depends on leveraging user data. Transparency in operations and conduct should be the industry norm. Independent researchers or government regulators should be afforded some ability to conduct tests on black box systems, audit networks, or otherwise assess the security of the mechanisms employed to gather, store, communicate, and secure sensitive information [2].

Legislation May Not Be as Effective as Regulation

Heavy-handed legislation tied to specific-technologies could stifle competition and innovation or quickly become obsolete. If poorly constructed, the imposed measure could even be turned to serve conniving tech giants as shields against consumer complaints or future legislation [2]. Transparency and control provisions should not be used to undermine or censor free speech in digital domains. Disclosure rules must protect user anonymity. User rights to own or control their data should not be allowed to encapsulate restrictions on what others say about a user. A free and open Internet depends on respecting the rights of all users and promoting the open access to factual information; especially when that content is vital to the public defense against false narratives [2]. Instead of responding to a single incident while hundreds of others occur on a daily basis, regulators, such as the FTC, can codify inalienable consumer privacy rights that strike at the disease of dragnet surveillance capitalism.

ICIT Contact Information

Phone: 202-600-7250

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

Sources

[1] Williams, J. (2018). *'Scraping' Is Just Automated Access, and Everyone Does It*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2018/04/scraping-just-automated-access-and-everyone-does-it [Accessed 25 Apr. 2018].

[2] McSherry, C. (2018). *Data Privacy Policy Must Empower Users and Innovation*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2018/04/smarter-privacy-rules-what-look-what-avoid [Accessed 25 Apr. 2018].

[3] Gebhart, G. (2018). *To #DeleteFacebook or Not to #DeleteFacebook? That Is Not the Question*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2018/04/deletefacebook-or-not-deletefacebook-not-question [Accessed 25 Apr. 2018].

[4] Kfvs12.com. (2018). *No punishment for Equifax after massive hack*. [online] Available at: http://www.kfvs12.com/story/38009312/no-punishment-for-equifax-after-massive-hack [Accessed 25 Apr. 2018].

[5] Varian, H. (1996). *Economic Aspects of Personal Privacy*. [online] People.ischool.berkeley.edu. Available at: http://people.ischool.berkeley.edu/~hal/Papers/privacy/ [Accessed 25 Apr. 2018].

[6] Newsweek. (2018). *Did you delete Facebook? Mark Zuckerberg didn't notice.....*. [online] Available at: http://www.newsweek.com/zuckerberg-says-deleting-facebook-has-no-meaningful-impact-his-business-872876 [Accessed 25 Apr. 2018].

[7] Parkin, S. (2018). *Has dopamine got us hooked on tech?*. [online] the Guardian. Available at: https://www.theguardian.com/technology/2018/mar/04/has-dopamine-got-us-hooked-on-tech-facebook-apps-addiction [Accessed 25 Apr. 2018].

[8] Pollach, I. (2007). *What's wrong with online privacy policies?*. [online] Researchgate. Available at: https://www.researchgate.net/publication/220421895_What's_wrong_with_online_privacy_policies [Accessed 25 Apr. 2018].

[9] Statista. (2018). *Worldwide average daily time spent online 2017 | Statistic*. [online] Available at: https://www.statista.com/statistics/736727/worldwide-teen-average-online-time-devices/ [Accessed 25 Apr. 2018].

[10] McDonald, A. and Cranor, L. (2008). *The Cost of Reading Privacy Policies*. [online] Lorrie.cranor.org. Available at: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf [Accessed 25 Apr. 2018].

[11] Facebook.com. (2018). *Accessing Your Facebook Data | Facebook Help Centre | Facebook*. [online] Available at: https://www.facebook.com/help/405183566203254/ [Accessed 25 Apr. 2018].

[12] Schneier, B. (2018). *It's not just Facebook. Thousands of companies are spying on you*. [online] CNN. Available at: http://It's not just Facebook. Thousands of companies are spying on you [Accessed 25 Apr. 2018].

[13] Washington Examiner. (2018). *Equifax says it's still under CFPB investigation*. [online] Available at: https://www.washingtonexaminer.com/equifax-says-its-still-under-cfpb-investigation [Accessed 25 Apr. 2018].

[14] Brown, J. (2018). *A Data Protection Officer's Guide to the GDPR Galaxy*. [online] Dark Reading. Available at: https://www.darkreading.com/endpoint/a-data-protection-officers-guide-to-the-gdpr-galaxy-/a/d-id/1331262 [Accessed 25 Apr. 2018].

[15] Kjensrud, R. (2018). *How GDPR Forces Marketers to Rethink Data & Security*. [online] Dark Reading. Available at: https://www.darkreading.com/risk/compliance/how-gdpr-forces-marketers-to-rethink-data-and-security/a/d-id/1331475 [Accessed 25 Apr. 2018].

[16] Sheridan, K. (2018). *Securing Social Media: National Safety, Privacy Concerns*. [online] Dark Reading. Available at: https://www.darkreading.com/vulnerabilities---threats/securing-social-media-national-safety-privacy-concerns/d/d-id/1331594 [Accessed 25 Apr. 2018].