Validating Privacy Requirements for the Personal Data Trade:

Lessons from the Sarbanes-Oxley Act of 2002

By: Terrence R. Cahill, CPA, CISA
EMCS: Class of 2019

BROWN
School of Professional Studies

Table of Contents:

Overview:

Executive Summary

As tens of thousands of companies in the United States monetize the collection, analysis and sale of personal data in the United States, the existing patchwork of data privacy laws is not enough to ensure its confidentiality. This paper examines those existing laws, recent data breaches and the surreptitious industry that has grown in spite of, around and between the cracks of the current requirements - the consumer reporting, data broker and ad-tech industries. In addition, this paper also analyzes catalysts that led to the implementation of the Sarbanes-Oxley Act of 2002, draws parallels to the current environment facilitating the data trade, and makes inferences on whether similar reforms could be as effective in maintaining the confidentiality of non-public personal data across all industries in the United States.

Problems Addressed

Nearly 70% of United States Gross Domestic Product ('GDP') comes from consumer spending which incentivises businesses to obtain as much data on consumers as possible to extrapolate future behavior, preferences, etc. whether we have a relationship with them or not. The mixed federal privacy requirements by industry (healthcare, credit reporting, financial, etc.) has not kept pace with the innovation from those that most profit from it's collection, analysis and trade - consumer reporting agencies, data brokers and the ad-tech industry. As large amounts of personal data is correlated and concentrated by these companies, they become especially attractive targets for nefarious actors. In the current environment, most of these companies do not answer to the individuals in which they profit from, and consumers have little to no recourse if there is a breach or major trust violation.

Solution Proposed

Those companies that trades and/ or profits from the sale of personal data (e.g. Google, Facebook, Mastercard, Equifax and so on) unless it is sufficiently de-identified, should be required to 1) demonstrate annually to an independent auditor, the effectiveness of several "minimum necessary" internal control objectives around privacy for brokered personal data, and 2) provide executive sign off on the design and operation of the controls that satisfy those objectives. Furthermore, a new oversight board or federal standards council should be established to regulate, inspect and discipline the firms that perform the assessments and specific civil penalties should be defined for negligence, fraud, material misrepresentation and other abuses with the transfer or sale of personal data, regardless of type.

State of the Art Approach Pursued

The objective of this Critical Challenge Project is to conduct research and analysis on the current state of the market and to conclude on best practices to ensure the confidentiality of personal data within and across the budding data trade industries. The approach taken has been to apply the practices utilized and perfected by financial compliance and internal control auditing to the realm of privacy regulations to demonstrate how these practices will better ensure action by these high-risk companies and protection of consumer personal data.

Introduction

In conjunction with the world's increasing reliance on smartphones and influence of social media, surveillance capitalism is quietly becoming one of the most powerful and

influential business models for the 21st century. Most of us have some vague notion that companies and services we use online are using the data we share to show us more relevant advertising, search results, coupons, things related to our interests and to help us make connections across our social networks. More connections lead to increased engagement with the platform and thus more advertising opportunities. A lot of these services such as Gmail and Facebook are free to use and improve our lives in various ways. Ad's themselves can be annoying but they are for familiar products and services and most of us learn to ignore them. Ostensibly, it sounds like a fair trade, relatively benign and most people don't think twice about signing up.

However, what about the companies that build profiles on us that we don't have a relationship with? Or the companies that collect data from our phones instantly when we open another completely unrelated app? How about when these various services (online and offline) collaborate with each other, consolidate their data and sell or trade it for profit, and can then use it to exploit or make preemptive judgements and decisions that affect our lives such as political campaigns, insurance companies, healthcare providers, credit companies, law enforcement agencies and other government entities? Furthermore, what about when the data used to score, rate and risk-rank our profiles is inaccurate or incomplete? What is acceptable and what isn't? It is difficult to pinpoint where exactly the line of immorality was crossed and who was responsible, but one thing's for sure, it was crossed years ago and right under our noses.

Over the last decade especially, the variety, quantity and quality of consumer personal data has exploded as companies demand more granular data about consumers and employ increasingly invasive methods of collecting and trading it. Shadow profiling, browser fingerprinting, web scraping, e-mail scanning, and web beacons are just a few of the questionable methods used to gather data about us which includes everything from geolocation

data, browsing history, online transactions, lifestyle choices, behavioral data, and so on. What actions should be required of these companies (beyond the commonalities of existing privacy laws) to ensure that they are sharing and trading this data responsibly and taking adequate steps to protect it? A clear legislative line needs to be drawn between the data we choose to share with certain people/ platforms and data that is obtained and inferred about us and traded/ sold outside our sphere of influence and without our knowledge. Providing convoluted, lengthy privacy policies are not enough[1]. Furthermore, it stands to reason that applying historical lessons learned for similar scenarios could provide a head start on addressing the problem.

This report analyzes existing federal privacy laws and the industries largely responsible for the personal data trade - consumer reporting agencies, data brokers and ad-tech companies in the United States. Where innovation has outpaced legislation, this report lays out clear steps that can be taken to tip the scales back in favor of U.S. consumer privacy and to help prevent future abuses and restore confidence based on similar historical conditions, enacted legislation and existing data thereof. In addition, the appendices 1) contain a proposed "minimum necessary" control framework that should be required of any company that collects, analyzes, packages, distributes and/ or resells personal data for profit and demonstrate compliance with on an annual basis, 2) document a list of resources individuals can leverage and tools they can use to lessen the impact of the consumer reporting/ data broker/ ad-tech chokehold they already have on each of us, 3) contains a visualization of the existing U.S. privacy laws for high-level compare/ contrast analysis, and 4) a list of open-source tools that a company can use to demonstrate compliance with the proposed "minimum necessary" control framework in #1 above. It is also the author's hope that this report will increase awareness of these insidious industries and help shape the discussion around future U.S. Federal Privacy Law.

[1] Consumerist article on privacy policies.

Background

The “Problem” Industries

Given that nearly 70% of the U.S. GDP is consumer spending[2], and as of 2016, adults in the U.S. spend nearly 11 hours per day using electronic devices[3], there is both an increased availability and demand for increasingly granular data about consumer preferences, choices, ability to spend and other demographic data. Advertising is shifting from the traditional “stimulus-response” model (passive advertisements in hopes that a broad group of people see identify with, and maybe buy) to targeted personal advertising enabled by mobile devices. The standard now is to predict what specific individuals want or need with real-time data before they even know, and encouraging interaction with the content and sharing their purchases with others. Advertising technology companies like Google-owned DoubleClick, Facebook, Adobe, Amazon and Criteo have facilitated this shift and have become a major factor in the modern economy with privacy implications being largely an afterthought. Another example is ad-tech company Civis Analytics which helped get President Obama re-elected in 2012. It used proprietary methods and algorithms to combine voter data and other viewership data and provided the campaign a “a vastly more detailed blueprint of what types of people were watching what, when”[4] and eliminated a lot of unnecessary spending. It is forecasted that digital advertising will grow 10% per year through 2020.[5]

The consumer reporting industry is made up of over four hundred agencies in the United States, including the “big 3” (Equifax, Experian and TransUnion) and has been around since the 1800’s. They primarily “collect and sell personal consumer information, such as banking

[2] St. Louis Fed Chart.
[3] Scripps health article.
[4] Wired Article.
[5] AdExchanger Article.

histories, health data, medical payments, tenancy, employment, and insurance claims."[6] Although data brokers are technically separate from consumer reporting agencies, they operate the same way with the same processes and even use and exchange most of the same data amongst each other. It is not known exactly how many data brokers exist, but credible estimates from mid-2016 indicate anywhere from an additional 2,500 to 4,000 are in operation in the United States.[7] The data broker industry is expected to grow at a compound annual growth rate of 11.5% for the next ten years and as expected, the softly regulated market and consumer spending mecca of the globe, North America is expected to be the most active and lucrative market.[8]

The ad-tech and consumer reporting/ data broker industries work together, along with traditional companies (e.g. Mastercard) to exchange, consolidate, analyze and sell consumer data to everyone from hedge funds to political campaigns[9]. All these companies together (including location aggregators) would commonly be classified as "data miners" and there are two variants of these: first-party and third-party. First-party data miners are ones in which 1) people voluntarily engage with and provide data to as part of, or in exchange for a service for a reduced fee (or no fee) and 2) consumers have a choice not to continue utilizing that company/ service (such as Google). Third-party data miners are those in which citizens have little-to-no interaction with the companies and are largely unaware of their existence (such as Equifax or any data broker).[10]

Existing Laws in the United States

[6] List of nationwide specialty consumer reporting agencies article.
[7] Newsweek article - "Very little oversight"
[8] Market research hub article.
[9] Forbes article.
[10] EFF article on vermont data broker law.

As a response to this mass data collection and exchange, governments across the globe have been racing to implement new comprehensive data privacy laws and establish new rights for their citizens (a.k.a. “data subjects”) and requirements for handling personal data. The European Union set the bar in terms of breadth and scope with the General Data Protection Regulation (‘GDPR’) effective May, 2018 which applies to any company that processes data for an EU citizen. Numerous other governments followed closely behind with comparable laws such as Brazil, Canada, Singapore, South Korea and even Mexico. Even the State of California has established their own flavor of consumer privacy protections - the California Consumer Privacy Act (‘CCPA’) set to be enforceable for California companies as of January 1, 2020.

CCPA is a great first pass at a comprehensive consumer protection privacy law and will do a lot of great things such as encouraging transparency in businesses that handle personal data, requiring a quicker notification to consumers for data breaches, setting security and protection requirements over personal data and legally defining data processing, personal data and other critical terms. It even grants new rights to data subjects including the right for disclosure, right to deletion, right to access, right to rectification, right to opt-out, and even the rights of non-discrimination.[11] While most everyone agrees that these are noble intentions and will greatly benefit citizens in California, CCPA does not specifically address or target third-party data mining and will likely do little to actually curb the data trade.

Credit reporting agencies are governed by the Fair Credit Reporting Act (‘FCRA’), enacted in 1970 and updated in 2003 by the Fair and Accurate Credit Transactions Act. According to Investopedia, the FCRA “defines the permissible purposes for obtaining a consumer credit report, standards for information that should be included on a credit report,” length of time entries can remain on one, and allows consumers to know what’s in their file,

[11] https://www.varonis.com/blog/ccpa-vs-gdpr/#_

receive a free copy once per year (if consumers somehow find the website and jump through the necessary hoops), verify accuracy when required for employment, notification when an item has been used against them, and dispute/ correct information that is inaccurate or incomplete[12]. Unsurprisingly, the FCRA "generally does not cover the sale of consumer data for marketing and other purposes"[13] which is one reason the data broker industry has been exploding. Also, the FCRA was written almost fifty years ago, long before web-scraping, browser fingerprinting, http cookies[14] and the proliferation of online shopping, social media, web browsing, and near instant exchange of mass quantities of digital data with thousands of elements about our lives.

Although the U.S. Federal Government isn't far from implementing their own comprehensive privacy law (the most recent draft bill was submitted to the Senate in late 2018), in the meantime consumers must rely on a various patchwork of state laws and assortment of various federal rules that have been tacked on to decades-old laws. The U.S. has federal privacy protections for healthcare (Health Insurance Portability and Accountability Act ('HIPAA')), the financial industry (Gramm-Leach-Bliley Act ('GLBA')), children under the age of 13 (Children's Online Privacy Protection Act ('COPPA')), credit reporting (Fair Credit Reporting Act ('FCRA')), and for personal data collected by state motor vehicle departments (Driver's Privacy Protection Act ('DPPA')). It might seem like the essentials are covered, but in general they are ambiguous, lack oversight and an effective validation/ enforcement mechanism. With the exception of HIPAA, these are administered and enforced by the Federal Trade Commission ('FTC'), which was established in 1914, and Consumer Financial Protection Bureau ('CFPB'), established in 2011 (authority and enforcement will be discussed in a section below). HIPAA is enforced by the Department of Health and Human Services ('HHS') which was established in

[12] Investopedia article FCRA.
[13] FTC report on Data Brokers
[14] See Appendix B for more details on invisible data collection methods.

1953. (For a high-level overview and comparison of each of these existing laws, please see the spreadsheet attached in Appendix D).

Only one body has managed to pass legislation thus far specific to data brokers - the State of Vermont. According to the Vermont Data Broker Accountability and Transparency Act (H.764) signed into law in mid-2018, and effective as of January 1, 2019, a "'data broker' is a business, or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship."[15] A few key items of note about the Vermont law is that it does not require the data brokers to provide an opt-out for consumers, does not require consent, or require a mechanism to address inaccurate or incomplete data. It does however "require data brokers to register with the Secretary of State" annually (and file a $100 fee), requires data brokers to "adopt an information security program with appropriate technical, physical, and administrative safeguards", prohibits the acquisition of personal information "with the intent to commit wrongful acts", and "prohibits credit reporting agencies from charging a fee to place or remove a credit freeze." It does little to actually help or educate consumers, and like other federal privacy laws, leaves too much room for interpretation over what constitutes "appropriate technical, physical and administrative safeguards". It essentially just scratches the surface and leaves a lot to be desired in regulating the data trade.

Problems

Transparency

15 https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf

In 2014, the FTC released a detailed report ("Data Brokers: A Call for Transparency & Accountability") on an in-depth study of nine data brokers "representing a cross-section of the industry" to examine their processes and practices. "Data collected could include bankruptcy information, voting registration, consumer purchase data, web browsing activities, warranty registrations, and other details of consumers' everyday interactions. Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers even exist and are collecting and proliferating this information. While each data broker source may provide only a few data elements about a consumer's activities, data brokers pull all of these data elements together to form a detailed composite of the consumer's life."[16]

The FTC report found that "data brokers collect and store billions of data elements covering nearly every U.S. consumer"; One out of the nine reviewed had an estimated 3,000 individual data elements on approximately 80% of the population obtained from both online and offline sources. "The extent of consumer profiling today means that data brokers often know as much – or even more – about us than our family and friends, including our online and in-store purchases, our political and religious affiliations, our income and socioeconomic status, and more," noted FTC Chairwoman Edith Ramirez in 2014, and one can only imagine how their capabilities have expanded in the five years since. The 2014 FTC report "unanimously recommended that Congress should consider enacting legislation that would enable consumers to learn of the existence and activities of data brokers and provide consumers with reasonable access to information about them held by these entities."[17]

Even with privacy protections in place over credit reporting companies and data breaches, a recent survey by Creditcards.com indicated that Americans still aren't taking

[16] FTC investigation of 9 data brokers https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf
[17] https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

advantage of the limited rights granted by FCRA and are not reviewing their credit reports or checking their credit score.[18] Credit reports are restricted in time and scope and do not provide a complete picture, so why then should a data broker with 3,000+ individual pieces of data about your life and preferences and more detailed and conclusive inferences with a broader impact not be subject to FCRA or even stricter requirements?

Tracking & Collusion

Online and offline, companies collect all kinds of data about us that we don't know we're sharing via cameras, cell phones, apps, browsers, loyalty programs, and all our other internet connected devices including, but not limited to, our newly internet-enabled home appliances. Operating systems for mobile devices and computers alike now essentially forbid anonymous use because their business model relies on collecting and monetizing your personal data. This constitutes the tracking that we are at least quasi-aware of. The really shady practices are done by companies like Google and Facebook which track and create profiles about you even if you opt out of their services. Even though you can technically delete your Facebook profile, you cannot always stop tracking as they can still collect data about you via your phone and browser and create a "shadow profile" for you through apps that use their software development kit ('SDK') used by companies like Kayak.com (the SDK defaults to automatically send data to Facebook instantly as the app is opened)[19]. In addition, to comply with GDPR, Facebook leaves the responsibility up to the app developer to obtain consent even though Facebook collects the data. In addition, Facebook actually purchases a significant amount of offline data from data brokers and other companies to supplement their online behavior tracking. "Facebook's 'Partner Categories' program, began licensing information from data brokers like Acxiom, Epsilon and

[18] CNN Americans still aren't checking their credit reports.
[19] How facebook tracks you on android.

Oracle Data Cloud to allow precision advertising targeting of its users based on the activities they perform offline or online outside of its walled garden."[20]

Location aggregators also have been outed numerous times for their abusive practices of buying consumer wireless location data from each of the major wireless companies and Google, and "reselling it to specific clients and industries"[21]. They were first exposed in early 2018, pledged to stop selling location data but exposed again in early January, 2019 when an investigator paid a bounty hunter $300 to locate a specific cell phone in Queens, NY[22]. The FCC stated that it would investigate this scheme in May, 2018[23] however the recent revelations indicate that the FCC hasn't been able to make much headway in the past eight months on this issue and that they either lack the personnel, resources, authority or will to intervene.

Incentives

Public companies are responsible to their investors and shareholders who demand a return on equity. The incentives to protect personal data are thus diametrically opposed to ours as they are paid immense amounts for user-specific data such as location data being sold by wireless companies, transaction data being sold to hedge funds, viewership data being sold to political campaigns, etc. Most companies want to collect as much data as they can and over the longest period of time as that enables them to better predict our future actions, and it's a steady income stream for them. There is no legal mechanism at the moment to require any company trading, selling or even just aggregating personal data be responsible to those whose data they trade.

[20] Data brokers so powerful article.
[21] Motherboard $300 bounty hunter article.
[22] TechCrunch article about new location aggregator scandal.
[23] Wyden article May, 2018 - Hunton privacy blog

Because they aren't accountable to the people who they profit from, they have little regard on whether the data they sell about you is even accurate. Some reports indicate that as little as 30% in as many as 1,500 unique data points about any given individual in the United States is actually correct.[24] A 50% accuracy rate is not uncommon[25]. Most of these companies even calculate proprietary "scores" on us (similar to credit reporting) with the inaccurate data elements, but about various other aspects of our lives and behavior, which makes them potentially just as effective. They do this because it makes their data more conclusive to buyers and thus, more valuable. In a recent investigation, examiners found that "the consumer reporting companies lacked good quality control to check the accuracy of their consumer records, were not following federal requirements, and found widespread problems with furnishers supplying incorrect information to the consumer reporting companies."[26] All these findings are for the relatively limited number of credit reporting companies that have been regulated by the FCRA since 1970; It is scary to think about the possible abuses, fraud, and manipulation occuring in the broader data broker market of 4,000+ companies.

Given the amount of power and money these industries have, and the vast implications of what the data can yield, lobbyists for these industries get paid tremendous amounts to kill legislation or regulatory power like they did with the 2016 FCC Privacy Rules that were stopped before they could be implemented[27]. If they know that they aren't likely to stop new legislation, these companies will instead devote their resources to influence, confine or weaken future legislation so it can work in their favor and even increase barriers to entry for future competitors in their market[28]. The New York Times recently reported that "in recent months, Facebook, Google, IBM, Microsoft and others have aggressively lobbied officials in the Trump

[24] How Data Mining Giant Got me Wrong Article.
[25] Newsweek article about Data Brokers.
[26] CFPB Oversight article.
[27] Forbes article - FCC rule nullification
[28] The Hill article - google releases privacy framework.

administration and elsewhere to start outlining a federal privacy law, according to administration officials and the companies. The law would have a dual purpose, they said: It would overrule the California law and instead put into place a kinder set of rules that would give the companies wide leeway over how personal digital information was handled"[29].

Notable Breaches/ Trust Violations

The mass sale and aggregation of data will attract more nefarious actors and identity thieves as the more information in one location yields the most useful data and allows almost anyone to reconstruct passwords, medical histories, financial accounts, etc. In June, 2018 the essentially unknown data broker "Exactis" may have exposed personal information of up to 340 million records. "(The unprotected, publicly accessible database) didn't include social security numbers or payment details, but goes into great detail for each individual, including interests, habits and the age and gender of children. It apparently included more than 400 variables ranging from religion, pets, whether a person smokes, to personal interests."[30] There is no concrete way of knowing who is part of the breach, and no recourse other than a class-action lawsuit. It's easier to just assume everyone with an online identity in the United States was compromised.

No one will soon forget the more publicized data breach, the Equifax data breach in late 2017 in which approximately 148 million people had their most sensitive information stolen and exposed to the depths of the dark web and weren't told for more than six weeks after the executives at Equifax knew. Social Security numbers, phone numbers, email addresses, dates of birth, financial account information and even driver's license numbers were compromised and those key personal identifiers cannot easily be changed like a credit card number can with your

[29] New York Times - On it's Own Terms Article.
[30] Exactis Breach - SecurityWeek Article.

bank. Also, the burden was left to the consumers to take remediative action to try and protect their identities and over a year later, there are still no penalties yet for Equifax or their executives. Furthermore, citizens still cannot opt-out of Equifax and they continue to grow and even profit from their security blunder by selling their "credit monitoring" services. Consumer reports noted in an editorial a year after the breach that "Equifax itself has suffered minimal consequences and continues to do business more or less as before" and even continues to receive large government contracts.

The Facebook/ Cambridge Analytica scandal of early 2018 is also fresh on the minds of U.S. citizens but unfortunately not well understood. A brief summary from the Atlantic Magazine indicated that "in June 2014, a researcher named Aleksandr Kogan developed a personality-quiz app for Facebook. It was heavily influenced by a similar personality-quiz app made by the Psychometrics Centre, a Cambridge University laboratory where Kogan worked. About 270,000 people installed Kogan's app on their Facebook account. But as with any Facebook developer at the time, Kogan could also access data about those users or their friends. When Kogan's app asked for that data, it saved that information into a private database instead of immediately deleting it. Kogan provided that private database, containing information on as many as 87 million Facebook users, to the voter-profiling company Cambridge Analytica. Cambridge Analytica used it to make 30 million "psychographic" profiles about voters."[31] The important thing to note was that this wasn't a "breach", it was simply a massive trust violation and lack of oversight/ control by Facebook. There isn't a legal mechanism in place currently that would prevent something like this from happening again other than nebulous corporate privacy policies. It shouldn't matter what kind of company is trading this type of data (voter profiling companies, wireless companies, internet service providers, credit card companies, data brokers, credit reporting companies, ad tech companies, etc.), the lesson here is that where

[31] The Atlantic magazine article - cambridge analytica synopsis.

personal data is being traded and not de-identified, it should have validation requirements which is not afforded under CCPA or even GDPR.

Gaps & Limitations of Enforcement

Aside from the obvious gap of the U.S. not yet having a federal privacy law, there are other issues with current oversight and enforcement. Most of the current federal laws, with the exception of HIPAA, are enforced by the Federal Trade Commission ('FTC') or the Consumer Financial Protection Bureau ('CFPB'). The FTC is considered a regulator while the CFPB is considered a supervisory entity. Primarily, consumers have to submit complaints to these bodies which requires a large budget for staff and time for thorough investigations. Between the two entities, there appears to have been a lot of initial confusion between which entity needed to take the lead in investigating and probing Equifax. "Regulators do not conduct investigations and exams concurrently, because investigators would be able to get privileged information that supervisors could not, creating problems. As a result, the CFPB's examination of Equifax likely was put on hold while the FTC's investigation moved forward"[32]. It is not immediately clear which entity would investigate data trade abuses as they arise in the future. The CFPB became the overseer of the consumer reporting industry in 2012, but complaints about the industry are still near all-time highs. If the upcoming Federal Privacy Law doesn't include civil penalty authority for the FTC (which would allow it to fine companies), it would affect their ability to really impact behavior on a broader scale. "The FTC was created to be broad and general, affording it flexibility in handling cases. The commission doesn't have fining authority until clear lines are drawn regarding what a violation is"[33] and those lines are not in place yet.

[32] American Banker article about CFPB and Equifax.
[33] FTC Punching above it's weight article.

For data brokers, current enforcement capabilities largely rest on Section 5 of the Federal Trade Commission Act, which "prohibits unfair or deceptive acts or practices; The mere existence of (a data broker) site is not necessarily a violation, the site needs to make misleading statements or commit an act that causes injury to consumers"[34] which they often don't do. As for in-depth FTC studies and investigative reports, the FTC can release a comprehensive report and study about data brokers like they did in 2014, but the legislature doesn't need to actually follow any of those recommendations, which has been precisely the case. Based on the draft "Data Care Act" that was submitted in September, 2018, nothing from the FTC's investigation or previous comments were considered in it's writing.

"The FTC has acted as the technology and cybersecurity watchdog of the government for the last several years. The growing power of the technology industry and the impacts of massive data breaches are pushing the commission to reevaluate its regulation of the industry and the use of personal data."[35] The FTC fined Google $22.5 million in 2012 related to a misrepresentation of setting cookies on Apple's Safari browser, but that represented about .04% of their revenue for that year ($50.2 billion) - essentially a drop in the bucket that wouldn't have a meaningful impact on behavior. As of mid-January, 2019, the FTC is considering a "record fine" for Facebook privacy violations but will likely be immaterial for the company like the Google fine. In addition, the FTC's current "staff level is 50 percent below its level at the beginning of the Reagan administration in 1981"[36] and with the growth in population and the size of the federal register, this is an alarming number. Expecting the FTC to effectively enforce a new federal privacy law is set up for failure.

[34] Motherboard article - what are data brokers.
[35] FTC Punching above it's weight article.
[36] Govtech - FTC Asks for more over big-tech Article.

“Privacy Fatigue”

It is not reasonable for consumers to have to read tens of pages of legalese in every company’s privacy policy to determine who their personal data is being shared with. Most users simply don’t read them, but even the ones that attempt it are usually quickly overwhelmed by all the caveats, complex language, conditions, and sheer length. A few privacy regulations require “clear” or “plain english” privacy policies (COPPA, GLBA, HIPAA and GDPR specifically) but those instructions have different meanings to different people, depending on a variety of factors. The pace of change in the industry also renders a thorough read almost useless as companies frequently contract with new partners or develop new ways of tracking and packaging personal data. Privacy policies are not often written for individual users, they are written for the protection of the company and users often have to accept the terms regardless of their desires in order to use the services - it's often a “take it or leave it” approach across the board. There are a few AI tools that have been created[37] to try and extract the actual information from privacy policies but users shouldn’t need specialized tools like that to be able to understand where their data is going and how it's being protected. (For a list of tools to help with this and other privacy concerns, see Appendix A below).

Privacy fatigue is a relatively simple concept to grasp but has surprisingly little empirical data collected about it. One study from April, 2018 concluded that “increasing difficulty in managing one's online personal data leads to individuals feeling a loss of control. Additionally, repeated consumer data breaches have given people a sense of futility, ultimately making them weary of having to think about online privacy”[38]. After surveying over 300 internet users, their analysis showed that “privacy fatigue has a stronger impact on privacy behavior than privacy

[37] Wired article about privacy policies.
[38] Science direct article - privacy fatigue

concerns do, although the latter is widely regarded as the dominant factor in explaining online privacy behavior"[39].

Once you get past the sheer number of various privacy policies that are impacting each of our lives on any given day, the actual act of opting-out requires a user to submit even more identifying information where as an opt-in only system would eliminate that need. A similar scenario occurred with the Equifax breach: "The site the company set up for consumers to check if they were affected by the breach asked for six digits of the visitor's Social Security number, then told people their data was exposed no matter what they entered. The website itself was also vulnerable to hacking, not that it really mattered all that much seeing as Equifax sent people to a phishing site set up to look just like the real one"[40]. Half-hearted or hasty solutions implemented by these companies can and will create other similar issues for future breaches. This is an obvious problem that laws like GDPR and CCPA won't help mitigate, but having a requirement of internal controls validation would.

Proposed Solutions

Internal Controls Validation

Internal control requirements, and the validation thereof, would go a long way in ensuring that any business that collects, analyzes, packages, trades and/ or profits from the sale of consumer personal data that is not sufficiently de-identified, is taking the appropriate steps to comply with the law, has enough resources to perform the required actions and are actively engaged in protecting the confidentiality of personal data. The Committee of Sponsoring Organizations ('COSO'), established in 1985, defines "Internal controls" as a process "effected

[39] Science direct article - privacy fatigue
[40] Gizmodo article about equifax operating another credit bureau.

by management and other personnel, and those charged with governance, and designed to provide reasonable assurance regarding the achievement of certain objectives". Internal controls allow flexibility in how management addresses the requirements (control objectives) in any given framework while at the same time ensuring ongoing or periodic processes or activities are operating and designed effectively to address the associated risks. Internal controls can be broad or very specific, can be improved/ tweaked over time, and are also scalable depending on the size and operational reach and infrastructure of a business. They also increase Audit Committee and executive involvement in processes, help improve and standardize compliance documentation and processes for other laws and help minimize human error.

A few months after the Equifax breach was announced, the company signed a consent order that included reasonable but significant IT audit mandates with eight states. Among other things, "the order includes a provision to beef up its internal audit program. It requires better assessments of internal IT controls, with frequent scans of high- and medium-risk systems. It also requires audit committee monitoring of all findings identified by internal audit. The board also must bolster oversight of the audit function and approve a written risk assessment identifying foreseeable threats to the confidentiality of personally identifiable information."[41] These new requirements will be very effective in ensuring the security procedures for Equifax are at a minimum level and that there are preventative measures in place for the future. If internal controls are identified as an acceptable solution/ response by eight states in the most egregious data breach in American history, then some version of these requirements should be required of all high-risk data trade businesses.

Parallels to Accounting Fraud Environment of 1990's

[41] Internal audit 360 article.

The dramatic increase in the data trade and related breaches in recent years in some way parallels the increase in off-balance sheet entity use and other accounting scandals (namely Enron and WorldCom) in the 1990's that led to the passage of the Sarbanes Oxley Act of 2002 ('SOX'). Companies were taking advantage of complex and esoteric concepts, limited consumer insight and loopholes that few people understood to hide activity that they knew was predatory and manipulative. Although these companies had auditors, prior to SOX there was no central oversight board for the audit firms, limited governance, transparency or accountability requirements, no criminal penalties for executives who "cooked the books" and no internal controls validation requirement. Although SOX does raise compliance costs, it has had a positive impact on corporate accountability and investor confidence (at least as it pertains to financial reporting). A 2017 study published by the American Accounting Association "provides evidence that the requirements SOX set for financial reporting and public audits have, in fact, served as an extremely effective warning process in detecting corporate fraud."[42] If only we had a similar mechanism for privacy violations.

The U.S. Government Accounting Office released a comprehensive report in early September, 2018 which examined the Equifax breach and related response from both the company and the government and concluded that it occurred due largely to not keeping systems up to date, and "a lack of internal controls and routine security reviews."[43] In hindsight, an independent auditor tasked with the validation of privacy controls would have noticed the process gaps and likely noted that the CISO, given her music composition background, was not competent for that role however this type of conclusion was outside of the scope of the financial statement audit. The SEC has since updated their guidance (as of February, 2018) regarding "public companies' disclosure obligations under existing law regarding cybersecurity risk and

[42] The Balance Article - Enron, Corp. Fraud & SOX.
[43] Equifax data breach - one year later article.

incidents."[44] As a professional IT Auditor, it is not uncommon to see non-existent, weak and/ or understaffed privacy and information security programs and having a "minimum necessary" internal control framework to be independently verified is a reasonable, prudent solution to a problem that has gotten out of hand. Furthermore, as more infrastructure moves to the cloud, this audit requirement becomes less burdensome because businesses (and their auditors) can rely on their vendor controls, which mostly already produce widely accepted and utilized 'SOC' reports.

SOC reports, or 'System/ Service and Organization Control' reports are an independently produced audit report (by CPA firms) that a company can voluntarily have performed once per year (or how ever often they choose), instead of having all their customers attempt to perform the same audit or validation over their controls/ processes. SOC 2 reports are meant to be used by a companies clients/ customers and business partners and can already cover five "trust service principles": security, availability, processing integrity, confidentiality, and privacy. SOC 3 reports are relatively new and similar in form but meant for a broader audience and for use in marketing materials. SOC reports are easy to perform (and get easier each year), relatively inexpensive, scalable and customizable depending on the entity. They allow a company to establish their own processes (internal controls) to satisfy a minimum necessary listing of control objectives established by the American Institute of Certified Public Accountants ('AICPA') guidance.

Revisions and additional guidance for SOX a few years after implementation (the PCAOB's Auditing Standard #5) clarified that "both management and the external auditor are responsible for performing their assessment in the context of a top-down risk assessment, which requires management to base both the scope of its assessment and evidence gathered

[44] EY article about cyber disclosure requirements.

on risk". The FTC, AICPA, SEC, COSO, NIST, and various other privacy organizations could work together in the U.S. to establish the "minimum necessary" control objectives related to privacy and security for these high-risk entities and keep them current. (See Appendix C for a list of suggested "minimum necessary" control objectives for privacy within data trade industries).

Oversight

SOX isn't perfect by any measure, but it does a number of things right. First, it established the Public Company Accounting Oversight Board ('PCAOB') to set minimum audit standards and oversee the conduct of audit firms. SOX also required an annual review of the internal control structure around the generation of the financial statements and disclosures and required the executives to personally sign off on the financials and internal control effectiveness. This drives executive accountability, something that has been notably absent in recent data breach scenarios, namely the Equifax breach and Facebook leaks. After the passage of SOX, executives are held accountable for their actions (or inactions) and they take that very seriously. A data privacy/ information security internal control framework that needs to be positively certified quarterly by C-level executives, such as the CISO, CIO or CPO, would go a long way in driving accountability and decreasing the risks to the average citizen who currently has no knowledge of, or recourse against these companies that are trading their personal data.

Based on what is required by SOX as laid out by Wikipedia[45], IT leadership at all businesses that are involved in the collection and trade of personal data that hasn't been sufficiently de-identified should at a minimum be required to:

- Assess both the design and operating effectiveness of "minimum necessary" internal controls related to the privacy and protection of personal data,

[45] Wikipedia - SOX Act of 2002.

- Understand the flow of data, in sufficient detail to identify points at which higher risks for loss exist,
- Evaluate company-level (entity-level) controls, which correspond to the components of the NIST (or similar) framework around security and privacy of personal data,
- Perform an annual risk assessment,
- Evaluate controls designed to prevent or detect management override or circumvention of controls;
- Scale the assessment based on the size and complexity of the company;
- Conclude on the adequacy of internal control over the protection of personal data.

One positive aspect is that these audits would get easier to execute and validate year over year. For example, since most of the internal controls will be automated and system-based, auditors won't need to collect hundreds of samples like they do in financial audits; They can simply request, obtain and review the necessary system settings and ensure that they didn't change from the prior year. Processes will improve and a data privacy culture will build within the company starting at the executive level.

A bill was introduced to the House of Representatives in early January, 2019 that would "elevate the authority of the federal chief information officer and chief information security officer."[46] Assuming it passes and is implemented, it would be a good start for overseeing governmental entities and protecting their sensitive data, and may even strengthen the some enforcement mechanisms. However, even if it is passed, it will do little to protect personal consumer data held by thousands of public and private businesses. A new "bureau of personal data" or technology within the FTC could really be helpful in creating an oversight mechanism,

[46] Nexgov article - federal CIO authority.

setting minimum standards for personal data privacy, confidentiality and security across these industries and enable more effective enforcement for the existing and future laws.

Other Considerations/ Conclusion

Advertising technology and the personal data trade is important for a variety of reasons including mainly the “free” use of a lot of useful services and development of technologies that might not otherwise have existed. Secondly, advertising technology has developed some really innovative methods of identification, tracking, etc. that have useful applications outside of advertising. One example is the ability to identify or locate people based based on the scratches or dust spots on a camera lense[47]. Although most of us don’t like the idea when used to track or identify us, it could really be useful technology in trying to locate an abducted child or find a lost Alzheimer's patient, for example.

One great example of technology monitoring our behavior being a net benefit is in the auto industry. “Sensor technology in cars that watch and analyzes drivers, passengers and objects will mean enhanced safety in the short-term, and revenue opportunities in the future.”[48] Eye tracking technology can now warn about distracted driving and drowsiness and that data could be used to slow the car down or pull it over to the side of the road safely. It is important then not to limit and stifle ingenuity for these industries, but instead encourage anonymizing/ de-identifying it and limiting the nefarious uses by implementing some relatively easy methods to limit the oversharing of our personal data.

[47] Gizmodo article dust on camera lense.
[48] Reuters article about new driver monitoring tech.

Over the past two-decades, the internet has allowed almost anyone to start a business with a small investment and limited regulatory scrutiny. As this global marketplace matures, consumer privacy protections need to keep pace with the innovation that it has fostered. While a truly free market and educated populus will curb corporate oversharing of personal data across the broader market over time, regulation for the businesses involved in the unfettered personal data trade needs to be updated/ implemented in order to increase transparency and reduce harm to consumers in the short run. As these companies continue to innovate and collect data, consumers will always have to balance convenience and cost with privacy. We should create a system in which these businesses are forced to innovate on how to involve us and obtain our consent (such as paying us for using Facebook or providing paid subscription services for those who don't want their data shared). Deciding to sell or trade personal data without consent, knowledge or involvement by consumers, with little regard to its accuracy is where the line needs to be drawn.

Tim Cook, the CEO of Apple gave a speech in October, 2018 that warned of a "data-industrial complex" which was reminiscent of President Dwight D. Eisenhower's farewell address in 1961 warning us about the "military-industrial complex". Cook argued that private and everyday information is "weaponized against us with military efficiency, and that this mechanism doesn't just affect individuals, but whole societies. Platforms and algorithms that promised to improve our lives can actually magnify our worst human tendencies."[49] We've ignored Eisenhower thus far but we should do our best not to ignore Cook as data privacy issues are exponential, can't be undone and are very difficult to mitigate.

[49] The Verge - "Tim Cook Warns" article.

Appendix A: Helpful Links for Protecting Yourself Against Data Brokers & Ad-Tech

Data Mining Opt-Out List:
https://www.stopdatamining.me/opt-out-list/

Data Broker Identity Protection Paid Plans:
https://abine.com/deleteme/plans.php
https://www.infosweep.com/

How to Remove Yourself from Data Broker Sites:
https://motherboard.vice.com/en_us/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pipl-spokeo

Delete Facebook Guide:
https://www.nytimes.com/2018/12/19/business/delete-facebook-account.html

Delete Google Guide:
https://lifehacker.com/the-comprehensive-guide-to-quitting-google-1830001964

Tor Browser Information:
https://www.torproject.org/about/overview

Guide to Pi-Hole Network Ad Blocking:
https://www.myhelpfulguides.com/2018/07/15/install-pi-hole-raspbian-lite/

Browser Fingerprinting Analysis:
https://amiunique.org/
https://panopticlick.eff.org/

Privacy Tools:
https://amiunique.org/tools
https://www.privacytools.io/
https://prism-break.org/en/
https://realprivacy.io/

VPN & Email Guides:
https://thatoneprivacysite.net/

Privacy Policy A.I. Analysis for Ease of Understanding/ Visualization:
https://pribot.org/

Appendix B: Definitions and Details on Common Data Collection Schemes

Shadow Profiling - A term used to describe when companies collect data about your browsing habits, and other technical information about you or your device to create a "profile" about you even if you don't have an account with them usually via an app SDK default settings (3rd party tracking). See additional details here: https://media.ccc.de/v/35c3-9941-how_facebook_tracks_you_on_android
https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804

Web Beacons - Invisible or unobtrusive technique (usually a 1x1 clear .gif pixel) used by companies to determine if a user has accessed certain content (viewed a web page, opened or forwarded an email, etc.) (Can also be "like" or "upvote" buttons or similar). See additional details here: https://www.makeuseof.com/tag/how-web-beacons-track-web/
https://en.wikipedia.org/wiki/Web_beacon

HTTP Cookies - Small pieces of data added to your browser that assist with login features, preferences, personalized content and/ or track your behavior on the web. See more details here:
https://www.howtogeek.com/119458/htg-explains-whats-a-browser-cookie/

Canvas or Browser Fingerprinting - A technique used by companies to use the data about your specific browser (such as which plugins you have installed) and system settings (such as fonts, time zones, etc.) to uniquely distinguish you from all other visitors to that site. When 20+ categories of this information is added together, its ends up being very unique across the web and once the profile is built, it can be shared with other sites and ad networks. See additional details here:
https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers
https://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/#5e20fbcfa9bf

Web-scraping - A technique employed to automatically extract large amounts of data from websites whereby the data is extracted and saved to a local file in your computer or to a database in table (spreadsheet) format. See additional details here:
https://www.webharvy.com/articles/what-is-web-scraping.html

Pretexting - Pretexting is a form of social engineering in which an individual lies to obtain or misrepresents the reason for obtaining privileged data. A pretext is a false motive. Pretexting often involves a scam where the individual pretends to need information in order to confirm the identity of the person he is talking to. See additional details here:

https://www.techopedia.com/definition/13675/pretexting

E-mail Scanning -
The process by which a platform or 3rd party thereof, uses technology to scan the inbox and emails of users for keywords, events, dates, names, contact information and other potentially sensitive information.
https://money.cnn.com/2018/09/20/technology/google-gmail-scanning/index.html

Appendix C: “Minimum Necessary” Risk & Control Framework of Security and Privacy Internal Controls for Consumer Reporting Companies

See ‘Appendix C’ Spreadsheet.

Appendix D: Open-source Tools Small-to-Medium Sized Companies can use to help with Privacy Compliance Initiatives:

Privacy Impact Assessment:

Privacy impact assessment guide/ tool from the French Government:
https://www.cnil.fr/en/privacy-impact-assessment-pia

Pseudonymization:

ARX is a comprehensive open source software for anonymizing sensitive personal data:
https://arx.deidentifier.org/

Open Source standalone windows desktop application called OpenPseudonymiser by The University Of Nottingham:
https://www.openpseudonymiser.org/

Metadata Removal Tool:

Mat2 is a metadata removal tool, supporting a wide range of commonly used file formats:
https://0xacab.org/jvoisin/mat2

Project Management:

Open Source Project Management Software (GDPR Compliant):
https://www.openproject.org/

Open Source IT Governance Risk and Compliance Software:
https://www.eramba.org/

Open Source Identity & Access Management Tools:

Identity and Access Management Tools (including Privileged Access Management)
https://www.openiam.com/

Apache Syncope is an Open Source system for managing digital identities in enterprise environments, implemented in Java EE technology and released under Apache 2.0 license.
https://syncope.apache.org/
Internal Data Mining (classification, regression, clustering, association rules):
https://www.cs.waikato.ac.nz/ml/weka/index.html

General Privacy Tools by Category (email, instant messaging, etc.):
https://www.epic.org/privacy/tools.html

Appendix E: A Visualization and Overview of Current U.S. Privacy Laws:

See ‘Appendix E’ Spreadsheet.

Bibliography

"1-In-5 Internet Users Always Read Privacy Policies, But That Doesn't Mean They Understand What They're Reading." Consumerist. November 28, 2012. https://consumerist.com/2012/11/28/1-in-5-internet-users-always-read-privacy-policies-but-that-doesnt-mean-they-understand-what-theyre-reading/.

6, 2018 March. "Tips to Curb Screen Time for Adults." Scripps Health. March 22, 2018. https://www.scripps.org/news_items/6310-6-tips-to-curb-screen-time-for-adults.

Berry, Kate. "Is CFPB Punting on Equifax? It's Complicated." American Banker. February 05, 2018. https://www.americanbanker.com/news/is-cfpb-punting-on-equifax-its-complicated.

"CFPB Oversight Uncovers And Corrects Credit Reporting Problems." Consumer Financial Protection Bureau. https://www.consumerfinance.gov/about-us/newsroom/cfpb-oversight-uncovers-and-corrects-credit-reporting-problems/.

Cohan, Peter. "Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data." Forbes. July 24, 2018. https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/#17babe657722.

Cox, Joseph. "I Gave a Bounty Hunter $300. Then He Located Our Phone." Motherboard. January 08, 2019. https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

Cyber Thieves Could Use That Data to Open up Credit Cards. "Americans Still Aren't Checking Their Credit Reports." CNNMoney. https://money.cnn.com/2018/02/26/pf/credit-score-check-equifax/index.html.

Dayen, David. "Break Up the Credit-Reporting Racket." The New Republic. September 12, 2017. https://newrepublic.com/article/144780/break-credit-reporting-racket.

Dellinger, AJ. "Equifax Operates Another Credit Bureau, and You Can't Freeze Your Report

Online." Gizmodo. May 10, 2018. https://gizmodo.com/equifax-operates-another-credit-bureau-that-you-cant-fr-1825909532

"Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says." Fortune. http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/.

Grauer, Yael. "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?" Motherboard. March 27, 2018. https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

Greenberg, Andy. "An AI That Reads Privacy Policies So That You Don't Have To." Wired. February 09, 2018. https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/.

Hautala, Laura. "Federal Data Privacy Bill Introduced by 15 US Senators." CNET. December 12, 2018. https://www.cnet.com/news/federal-data-privacy-law-introduced-by-15-us-senators/.

Hickey, Alex. "'Punching above Its Weight,' FTC Needs More Rule-making Power, Resources, Commissioner Says." CIO Dive. October 03, 2018. https://www.ciodive.com/news/punching-above-its-weight-ftc-needs-more-rule-making-power-resources-c/538718/.

Hill, Kashmir. "Facebook Knows How to Track You Using the Dust on Your Camera Lens." Gizmodo. January 11, 2018. https://gizmodo.com/facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620.

Kagen, Julia. "Fair Credit Reporting Act (FCRA)." Investopedia. December 13, 2018. https://www.investopedia.com/terms/f/fair-credit-reporting-act-fcra.asp.

Kang, Cecilia. “Tech Industry Pursues a Federal Privacy Law, on Its Own Terms” New York Times. August 26, 2018. https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html

Konkel, Frank. "Lawmakers Reintroduce Legislation to Strengthen Federal CIO." Nextgov.com. January 04, 2019. https://www.nextgov.com/it-modernization/2019/01/lawmakers-reintroduce-legislation-strengthen-federal-cio/153945/.

Lammi, Glenn G. "The Nullification Of FCC's Broadband Privacy Rules: What It Really Means For Consumers." Forbes. April 12, 2017. https://www.forbes.com/sites/wlf/2017/04/12/the-nullification-of-fccs-broadband-privacy-rules-what-it-really-means-for-consumers/#58c49e4679ba.

Lapowsky, Issie. "The Tech That Got Obama Elected Will Now Fire Ads at You." Wired. June 30, 2017. https://www.wired.com/2015/10/civis-media-optimizer/.

Leetaru, Kalev. "The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong." Forbes. April 05, 2018. https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/#6f6d3dd73107.

"List of Nationwide Specialty Consumer Reporting Agencies." Know Your Health. https://www.annualmedicalreport.com/list-nationwide-specialty-consumer-reporting-agencies/.

Ma, Alexandra. "China Has Started Ranking Citizens with a Creepy 'social Credit' System - Here's What You Can Do Wrong, and the Embarrassing, Demeaning Ways They Can Punish You." Business Insider. October 29, 2018. https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

Market Research Hub. "Global Data Broker Market Industry Analysis Exhibits Progressive CAGR Growth of 11.5% During 2017 – 2026." SBWire. January 08, 2018. http://www.sbwire.com/press-releases/global-data-broker-market-industry-analysis-exhibits-progressive-cagr-growth-of-115-during-2017-2026-912175.htm.

Markey, and Edward. "Text - S.1815 - 115th Congress (2017-2018): Data Broker Accountability and Transparency Act of 2017." Congress.gov. September 14, 2017.

https://www.congress.gov/bill/115th-congress/senate-bill/1815/text.

"Massive Breach at Data Broker Exactis Exposes Millions of Americans." Information Security News, IT Security News and Cybersecurity Insights: SecurityWeek. https://www.securityweek.com/massive-breach-data-broker-exactis-exposes-millions-americans.

McCafferty, Joseph. "Equifax Consent Order Includes Internal Audit, IT Audit Mandates." Internal Audit 360. September 18, 2018. https://internalaudit360.com/equifax-consent-order-includes-it-audit-mandates/.

Menand, Louis. "Why Do We Care So Much About Privacy?" The New Yorker. June 22, 2018. https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy.

Meyer, Robinson. "The Cambridge Analytica Scandal, in 3 Quick Paragraphs." The Atlantic. October 26, 2018. https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/.

Neidig, Harper. "Google Releases Framework to Guide Data Privacy Legislation." TheHill. September 24, 2018. https://thehill.com/policy/technology/408145-google-releases-framework-for-data-privacy-legislation.

"New SEC Cybersecurity Guidance – Considerations for the Board." Home. https://www.ey.com/us/en/issues/governance-and-reporting/ey-sec-guidance-on-cybersecurity-board-considerations.

Peavler, Rosemary. "Enron, Corporate Fraud, and SOX." The Balance Small Business. https://www.thebalancesmb.com/sarbanes-oxley-act-and-the-enron-scandal-393497.

"Personal Consumption Expenditures/Gross Domestic Product Download." FRED. https://fred.stlouisfed.org/graph/?g=hh3.

Price, Dan. "5 Facebook Alternatives That Don't Steal Your Data." MakeUseOf. September 19, 2018. https://www.makeuseof.com/tag/facebook-alternatives/.

Ram, Aliya. "Data Brokers and Credit Scorers Accused of GDPR Breaches." Financial Times. November 08, 2018. https://www.ft.com/content/afef327a-e291-11e8-8e70-5e22a430c1ad.

Rotenberg, Marc. "Equifax, the Credit Reporting Industry, and What Congress Should Do Next." Harvard Business Review. September 20, 2017. https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next.

Sage, Alexandria. "Move Aside, Backseat Driver! New Tech at CES Monitors You inside Car." Reuters. January 09, 2019. https://www.reuters.com/article/us-tech-ces-monitoring/move-aside-backseat-driver-new-tech-at-ces-monitors-you-inside-car-idUSKCN1P219H.

"Sarbanes–Oxley Act." Wikipedia. January 09, 2019. https://en.wikipedia.org/wiki/Sarbanes–Oxley_Act.

Schwartz, Adam. "Vermont's New Data Privacy Law." Electronic Frontier Foundation. September 27, 2018. https://www.eff.org/deeplinks/2018/09/vermonts-new-data-privacy-law.

"Senator Wyden Calls for FCC Investigation into Company Sharing Location Data." Privacy & Information Security Law Blog. May 24, 2018. https://www.huntonprivacyblog.com/2018/05/24/senator-wyden-calls-for-fcc-investigation-into-company-sharing-location-data/#more-16345.

Snider, Mike. "ISPs Can Now Collect and Sell Your Data: What to Know about Internet Privacy Rules." USA Today. April 05, 2017. https://www.usatoday.com/story/tech/news/2017/04/04/isps-can-now-collect-and-sell-your-data-what-know-internet-privacy/100015356/.

Vincent, James. "Tim Cook Warns of 'data-industrial Complex' in Call for Comprehensive US Privacy Laws." The Verge. October 24, 2018. https://www.theverge.com/2018/10/24/18017842/tim-cook-data-privacy-laws-us-speech-brussels.

Weissbrot, Alison. "Zenith: More Money Goes To Ad Tech Than To Actual Media." AdExchanger. March 27, 2018. https://adexchanger.com/agencies/zenith-more-money-goes-to-ad-tech-than-to-actual-media/.

"What Is GLBA Compliance? Understanding the Data Protection Requirements of the Gramm-Leach-Bliley Act." Digital Guardian. September 19, 2018. https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act.

Whittaker, Zack. "Despite Promises to Stop, US Cell Carriers Are Still Selling Your Real-time Phone Location Data." TechCrunch. January 09, 2019. https://techcrunch.com/2019/01/09/us-cell-carriers-still-selling-your-location-data/.

[]. "FTC Asks for More Control Over Big Tech, Privacy Issues." Government Technology: State & Local Government News Articles. http://www.govtech.com/policy/FTC-Asks-for-More-Control-Over-Big-Tech-Privacy-Issues.html.

"The Role of Privacy Fatigue in Online Privacy Behavior." NeuroImage. December 05, 2017. https://www.sciencedirect.com/science/article/pii/S0747563217306817.