California Legislature

Senate Committee on Judiciary

HANNAH-BETH JACKSON
CHAIR

STATE CAPITOL
ROOM 2187
SACRAMENTO, CA 95814
TEL (916) 651-4113
FAX (916) 403-7394

INFORMATIONAL HEARING

THE SENATE COMMITTEE ON JUDICIARY

The State of Data Privacy Protection: Exploring the California Consumer Privacy Act and its European Counterpart

Tuesday, March 5, 2019
1:30 p.m.
State Capitol, Room 112

BACKGROUND PAPER

I. Introduction

In response to growing concerns about the privacy and safety of consumers' data, proponents of the California Consumer Privacy Act, a statewide ballot initiative, began collecting signatures in order to qualify it for the November 2018 election. The goal was to empower consumers to find out what information businesses were collecting on them and give them the choice to tell businesses to stop selling their personal information. In response to the pending initiative, which was subsequently withdrawn, AB 375 (Chau, Ch. 55, Stats. 2018) was introduced, quickly shepherded through the legislative process, and signed into law. The outcome was the California Consumer Privacy Act of 2018 (CCPA), Civil Code Section 1798.100 et seq.

The CCPA integrated many of the elements of the ballot initiative, which itself was inspired in part after the European Union's own regulatory scheme, the General Data Protection Regulation (GDPR). While the GDPR broke new ground in government response to rapidly evolving data collection and use practices, the CCPA represents what many consider to be the most robust consumer privacy law in the United States, albeit one of the only laws that addresses data collection and privacy holistically. Pursuant to the law, which takes effect in 2020, consumers have been granted a series of rights over their personal information. The CCPA provides consumers more control

over their information and a modest enforcement mechanism to protect some of those rights. Responsibility for enforcement falls almost entirely with the Attorney General. In addition, the Attorney General has also been tasked with issuing regulations to ensure clarity and the proper function of the CCPA.

In the rushed process to put together the bill, AB 375 included a number of issues that many agreed required immediate attention. SB 1121 (Dodd, Ch. 735, Stats. 2018) made largely technical and clarifying amendments to the CCPA with several more substantive changes sought by various stakeholders. In addition, a series of bills has already been introduced this session to further amend the CCPA. In anticipation of the Legislature's consideration of those bills, this informational hearing is intended to provide a more comprehensive look at the parameters of the CCPA; a comparison to other regulatory models, such as the GDPR; feedback on additional amendments necessary for the CCPA's effective implementation and operation; a sample of privacy-focused industry models; and a look at the Attorney General's role in ensuring the CCPA is operationalized and enforced. In addition, the hearing will provide an opportunity to delve deeper into how data is being collected, sold, used, and valued to better analyze and understand the current law and what more needs to be done.

II. The California Consumer Privacy Act: An Overview

The CCPA provides "consumers" certain rights regarding their "personal information" and places attendant obligations on "businesses" that touch that data.

A. Definitions

"**Consumer**" is broadly defined to include any natural person that is a resident of California. The definition of "**businesses**" contains two components. First, it must be a for-profit entity that does business in California, collects consumer information, and determines how to use that consumer information. Second, it must satisfy at least one of three thresholds:

- annual gross revenues in excess of $25,000,000;
- annually buys, receives, sells, or shares the personal information of at least 50,000 consumers, households, or devices; or,
- derives at least 50 percent of its revenues from the sale of consumers' personal information.

In addition, the law explicitly exempts certain entities and/or certain information collected by them, such as certain providers of health care and certain information collected by them; certain information collected by financial institutions; and certain information sold to or from consumer reporting agencies.

The CCPA defines "**personal information**" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." (Civ. Code Sec. 1798.140.) It provides a series of examples that constitute personal information if they identify, relate to, describe, are capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household, including:

- identifiers such as name, address, IP address, email, and other online identifiers;
- biometric information;
- browsing and search history; and
- geolocation data.

Personal information also explicitly includes any inferences that are drawn from other categories of personal information to create a consumer profile that reflects the consumer's "preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." It is not limited to information collected electronically or over the Internet. However, it explicitly does not include publicly available information, certain medical information governed by other laws, and information collected in connection with clinical trials.

This definition is fairly expansive, reflecting not only the many pieces of data that are personal to consumers but the ways in which that data is combined and utilized. Frequently, businesses draw their value from collected personal information by creating profiles of consumers reflecting their habits, patterns, preferences, political persuasions, and personalities and making inferences therefrom.

B. Rights

The CCPA grants a set of rights to consumers with regard to their personal information, including enhanced notice, access, and disclosure, the right to deletion, the right to restrict the sale of information, and protection from discrimination for exercising these rights.

Notice

The CCPA requires businesses to ***proactively*** notify consumers about the businesses' practices and the consumers' rights. They are required to include in any existing online privacy policies, or on their Internet Web site, a description of consumers' rights, methods for submitting requests, and a list of the categories of personal information it has collected, disclosed, or sold in the previous year.

Businesses are required to inform consumers at or before the point of collection about the categories of personal information to be collected and the purposes for which the

information will be used. Businesses are restricted from using that information for other purposes or collecting additional information without first providing relevant notice to consumers.

Disclosure

In addition to the affirmative duties on the part of businesses, the CCPA grants consumers the right to certain disclosures if a business collects information about the consumer, including:

- the categories of personal information it has collected about that consumer;
- the categories of sources from which the personal information is collected;
- the business or commercial purpose for collecting or selling personal information;
- the categories of third parties with whom the business shares personal information; and
- the specific pieces of personal information it has collected about that consumer.

Consumers have additional rights to disclosure in connection with ***information that is sold or disclosed for a business purpose***. Upon request, businesses must disclose to consumers the categories of personal information that the business collected, sold, or disclosed for a business purpose, and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

Access

Furthermore, the CCPA provides consumers the right to access the specific pieces of information collected about them. Businesses are required to promptly take steps to disclose and deliver the information without charge either by mail or electronically within a certain period of time, as specified.

These provisions do not require businesses to retain personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

The disclosures and access provided for above are only to be made available by businesses upon receipt of a "verifiable consumer request."

Restrictions on Sale

The CCPA provides consumers an extra layer of control over their data when it comes to the sale of the data. Consumers are given the ability to tell businesses to stop selling their information, if they are doing so, at any time. This right is referred to as the "***right to opt-out.***"

The CCPA requires each business to provide a clear and conspicuous link on its Internet homepage, titled "Do Not Sell My Personal Information." The link will connect consumers to an Internet Web page where a consumer, or a person authorized by the consumer, will be able to opt-out of the sale of the consumer's personal information. Businesses would then be required to wait at least 12 months before contacting the consumer to reconsider their decision to opt out. Businesses would be prohibited from selling the consumer's data until the consumer provides express authorization for such sale.
In addition to the notices discussed above, businesses are required to disclose in their privacy policies that the consumer's information may be sold, a description of the opt-out right, and a separate link to the opt-out Web page.

The CCPA provides stronger protections for certain minors. The CCPA provides that a business must not sell the personal information of consumers younger than 16 years of age without that consumer's affirmative consent (or, for consumers younger than 13 years of age, without the affirmative consent of the consumer's parent or guardian). This right is referred to as the right to "opt-in."

Right to Delete

The CCPA provides consumers the right to have certain personal information in the hands of businesses deleted. Consumers can request that a business "delete any personal information about the consumer which the business has collected *from* the consumer." Businesses are required to disclose this right, and if so requested, to delete the consumer's personal information from its records and direct any service providers to delete the information from their records, with certain exceptions.

There are a series of fairly broad exceptions wherein the business is not required to comply with such requests because retention of the information is necessary for certain purposes, such as:

- detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; or prosecuting those responsible for that activity;
- debugging to identify and repair errors that impair existing intended functionality;
- researching in the public interest;

- exercising free speech or another right provided for by law; and
- complying with a legal obligation.

There are also more open-ended exceptions to the right to deletion that are open to interpretation, such as where retention is necessary to "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" or to otherwise "use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."

Non-discrimination

The CCPA prohibits a business from discriminating against a consumer based on the consumer's exercise of the rights afforded in the CCPA. The provision includes a non-exclusive list of conduct amounting to discrimination:

- denying goods or services;
- charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- providing a different level or quality of goods or services to the consumer; or
- suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

However, within that same section and subdivision, the statute reads: "Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data." In the following subdivision, the CCPA authorizes businesses to provide "financial incentives" for the collection and sale of personal information. It also authorizes a business to offer "a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data." However, such practices require certain disclosures and consumer consent and must not be "unjust, unreasonable, coercive, or usurious in nature."

The language used in this section is contradictory at times, and it is unclear exactly what it allows and prohibits. For instance, it specifically lists "charging different prices" as prohibited discrimination, but then provides that nothing in the provision "prohibits a business from charging a consumer a different price." Additionally, it is unclear how "the value provided to the consumer by the consumer's data" would be measured, and by who.

Certainly, it is unknown how businesses, the Attorney General, or the courts will interpret these provisions. Fortunately, as discussed further below, the CCPA authorizes the Attorney General to establish rules and guidelines regarding these "financial incentive offerings" that may alleviate any confusion and avoid conflicting interpretations.

Limitations

In addition to those discussed above, the CCPA places specific limitations on the rights of consumers. The CCPA provides that the obligations imposed on businesses do not restrict a businesses' ability to:

- comply with federal, state, or local laws, or a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
- cooperate with law enforcement agencies concerning conduct or activity that may violate federal, state, or local law; or
- exercise or defend legal claims.

It also allows for the collection, use, retention, sale, or disclosure of consumer information if it is de-identified or in the aggregate. It also makes clear that the collection and sale of consumer information that takes place wholly outside of California is not restricted.

C. Enforcement

The CCPA provides two forms of enforcement: (1) limited private enforcement and (2) broader public enforcement under certain conditions by the Attorney General.

Private Enforcement

The CCPA provides consumers the right to bring a civil action for statutory and actual damages in only one context, when the consumer's non encrypted or non redacted personal information, as defined, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. Even before such an action can be brought, however, the consumer must provide the business 30 days written notice of the alleged violation (with certain exceptions) within which the business has the ability to cure the violation, where possible.

The CCPA further provides that nothing therein shall be interpreted to serve as the basis for a private right of action under any other law. Therefore, outside of the data

breach context, consumers are unable to directly vindicate their rights under the law. For instance, if a business is collecting the personal information of a child under 13 years of age without the parent or guardian's consent, the child and the child's parent or guardian would not have a remedy under the CCPA.

Public Enforcement

Outside of the above context, enforcement responsibilities are entirely the realm of the Attorney General. The CCPA provides that a business, service provider, or other person that violates the Act may be subject to an injunction and civil penalties in a civil action brought in the name of the people of the State of California by the Attorney General. It repeats that the civil penalties provided for are to be "exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General."

It should be noted that before the Attorney General can hold a responsible party accountable for a violation of the CCPA through a civil action, it must provide the alleged violator with notice of the violation and give the violator 30 days to cure any alleged violation. Essentially, a violation of the CCPA is not considered a violation of the CCPA until it remains uncured for 30 days from the point the Attorney General provides notice.

D. Attorney General Responsibilities

Outside of the broad enforcement duties discussed above, the Attorney General is charged with two main responsibilities, providing opinions and developing regulations.

First, the CCPA provides that "[a]ny business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of [the CCPA]." This provision may be interpreted to require the Attorney General to act as legal counsel for anybody that seeks it out in relation to CCPA compliance. Essentially, the very parties that may be in violation of the CCPA and that the Attorney General may be investigating, can seek legal guidance from the Attorney General regardless of the resources available to them.

Second, the CCPA tasks the Attorney General with soliciting broad public participation and adopting regulations to further the purposes of the CCPA. Such regulations must be adopted by July 1, 2020.

As part of their preliminary activities, the Attorney General's Office has conducted forums across the state to solicit public comment, both verbally in person or through

submitted written materials. It is posting transcripts from those forums on its Web site.[1] The Attorney General has indicated that the public should anticipate the publishing of a notice of proposed regulatory action in the fall of 2019.

The CCPA provides broad authority to the Attorney General. It provides a non-exclusive list of areas within which the Attorney General must develop regulations, including:

- updating categories of personal information;
- updating the definition of unique identifiers;
- establishing additional exceptions to the CCPA for businesses that are necessary for compliance with state or federal law;
- establishing rules and procedures for submitting and complying with consumer requests;
- developing a uniform opt-out logo or button;
- adjusting the monetary threshold in the definition of business;
- establishing rules, procedures, and exceptions to govern the notices and information provided to consumers;
- establishing rules and guidelines regarding financial incentive offerings; and
- establishing rules and procedures to govern verifiable consumer requests, with various goals, including the minimization of security concerns and the burden on both consumers and businesses.

In addition, the Attorney General is authorized to further adopt any additional regulations necessary to effectuate the purposes of the CCPA.

The regulatory role of the Attorney General is thus broad, complex, and ongoing. The goal is to operationalize the CCPA, the first of its kind and magnitude in the United States. While daunting, the regulatory authority provided for by the CCPA allows significant leeway for the Attorney General to iron out and clarify a number of the provisions of the CCPA that may be difficult to interpret and comply with. Clearly this will be particularly helpful with regard to the financial incentive provisions of the non-discrimination section and the security concerns around verifiable consumer requests expressed by industry stakeholders.

III. Other Regulatory Models: GDPR and Legislation across the States

A. General Data Protection Regulation: An Overview

[1] *California Consumer Privacy Act (CCPA)*, State of California Department of Justice, https://oag.ca.gov/privacy/ccpa [as of Feb. 27, 2019] (all further Internet citations have been visited as of February 27, 2019).

The Charter of Fundamental Rights of the European Union declares the following in regard to the protection of personal data:

- "Everyone has the right to the protection of personal data concerning him or her."
- "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."
- "Compliance with these rules shall be subject to control by an independent authority."

After years of negotiations and preparation, the General Data Protection Regulation (GDPR) was approved by the European Parliament and the European Council in April 2016, and became effective on May 25, 2018. The goals of the regulation were to modernize and harmonize European laws, protect and empower all EU citizens around their data privacy, and reshape the way organizations approach data privacy. It was a bold step toward effectuating the European Union's fundamental right to privacy and is widely considered the most robust privacy law in the world.
GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. It regulates "personal data," defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

In comparison to the CCPA, the GDPR has "controllers" rather than "businesses," "data subjects" rather than "consumers," and "processors" instead of "service providers." "Controller" is defined to mean "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." "Processor" is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

At its core, the GDPR takes a different approach to data protection than the CCPA. The fundamental principle underlying the GDPR is the requirement that a controller have a "legal basis" for *all processing* of personal data, otherwise processing is prohibited. The GDPR provides an outline of such bases, including consent, the necessity of the processing for performance of a contract, compliance with the law, or protecting the

vital interest of certain persons. The CCPA more narrowly focuses on the collection and transfer of data, and the general rule is that such processing is allowed.

The GDPR also requires certain controllers/processors to appoint a Data Protection Officer (DPO), including where there is large-scale data processing. The DPO must have expert knowledge of data protection law, be involved in all issues relating to the protection of personal data, and must not be given any instructions regarding the tasks assigned. There is also an explicit prohibition on retaliating against a DPO for carrying out their role.

In addition, there are different enforcement mechanisms. There is a much broader right of private enforcement under the GDPR as compared to the narrow right of action provided under the CCPA for data breaches.

The following chart provides a simplified comparison of what protections are provided under the respective laws. Although there are certainly differences in the approach of the laws, many businesses with GDPR compliance programs will have already incorporated many elements and processes necessary for compliance with the CCPA.

Consumer Rights/Protections	**GDPR**	**CCPA**
Broad Definition of Personal Information (PI)	Yes	Yes
Notice about Data Practices	Yes	Yes
Right to Access PI	Yes	Yes
Requires Specific Legal Ground for Processing PI	Yes	No
Requires Data Minimization	Yes	No
Data Portability	Yes	Yes
Right to Delete PI Consumer has Provided	Yes	Yes
Right to be Forgotten	Yes	No
Right to Correct Information	Yes	No
Right to Object to Automated Decision Making/Profiling	Yes[2]	No
Right to Object/Restrict PI Processing	Yes	Limited to Sales
Exclusion of Certain Categories of PI	No	Yes
Special Protection for Sensitive PI	Yes[3]	No
Public Enforcement	Yes	Yes
Private Right of Action	Yes	Limited (Data Breaches only)

[2] Article 22 of the GDPR provides: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

[3] Article 9 of the GDPR provides: "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." There are some exceptions, including where the data subject gives explicit consent but only where Member or Union state law allows for it.

B. Legislation in Other States

Since the passage of the CCPA, nine other states have introduced robust legislation to address data collection and privacy: Hawaii, Maryland, Massachusetts, Mississippi, New Mexico, New York, North Dakota, Rhode Island, and Washington. Nearly all of the bills are modeled after the CCPA, with various differences in the rights and protections afforded. One state, Washington, has a bill modeled heavily on the GDPR. It should be noted that at least six of the bills have private rights of action as strong, or stronger than California. Some, such as the bill in Massachusetts, provide for a private right of action for any violation of the law. The bills have been introduced by both Republican and Democratic lawmakers.

IV. The Importance of Data Privacy Protections

Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Privacy is therefore not just a policy goal, it is a constitutional right of every Californian. However, it has been under increasing assault.

A. History

The phrase "and privacy" was added to the California Constitution as a result of Proposition 11 in 1972; it was known as the "Privacy Initiative." The arguments in favor of the amendment were written by Assemblymember Kenneth Cory and Senator George Moscone. The ballot pamphlet stated in relevant part:

> At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian. The right of privacy . . . prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. . . . The proliferation of government and business records over which we have no control limits our ability to control our personal lives. . . . Even more dangerous is the loss of control over the accuracy of government and business records on individuals. . . . Even if the existence of this information is known, few government agencies or private businesses permit individuals to review their files and correct errors. . . . Each time we apply for a

> credit card or a life insurance policy, file a tax return, interview for a job[,] or get a drivers' license, a dossier is opened and an informational profile is sketched.[4]

In 1977, the Legislature reaffirmed that the right of privacy is a "personal and fundamental right" and that "all individuals have a right of privacy in information pertaining to them."[5] The Legislature further stated the following findings:

- "The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies."
- "The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."
- "In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

Although written almost 50 years ago, these concerns seem strikingly prescient. Today, the world's most valuable resource is no longer oil, but data. Companies regularly and systematically collect, analyze, share, and sell the personal information of consumers. While this data collection provides consumers various benefits, public fears about the widespread, unregulated amassing of personal information have only grown since privacy was made a part of California's Constitution.

B. The Consumer Benefits of Data Collection

The collection of personal information is used by businesses to customize digital services and content. Marketing is tailored to the finest detail. Consumers are introduced to products and services that they are more likely to be interested in as the relevance of advertisements clearly improves from the intricate profiles of consumers that are based on data from every facet of the consumers' lives. Industry advocates argue that broad data collection helps businesses thrive by maximizing their advertising dollars.

Data collection also assists with the development of language translation tools, mobile traffic services, digital mapping technologies, spell checkers, and other services consumers regularly rely on. The ability of businesses to capitalize on the collected personal information also provides the ability to provide certain services for free. Industry advocates argue that overregulation will undermine free services and content

---

[4] *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 17, quoting the official ballot pamphlet for the Privacy Initiative.

[5] Civ. Code Sec. 1798.1.

and stifle innovation. However, the control of this data by larger companies has given them enormous power, and the nature of what is collected, how it is collected, and what it is used for has drawn increased scrutiny.

C. The Tension Between Indiscriminate Data Collection and Privacy

With this widespread collection of data comes serious concerns about whether Californians' constitutional right to privacy is adequately protected.

IoT: The Internet of Things

Corporations are rapidly networking the physical world and gathering data from everything. Currently, everything from toasters and baby dolls to televisions and thermostats are connected to the Internet, gathering and using a wide range of information. This technology has limitless possibilities, and industry experts foresee a dramatic expansion in the years ahead. Recent research indicates that the number of such "smart" devices will climb to 25 billion by 2020.[6] The chief executive officer of Cisco has declared that IoT will generate $19 trillion in profits.[7]

However, many of these devices collect a vast amount of personal and intimate information. Arguably most disturbing, consumers may not even be aware of the full capabilities of these products or the information that is being collected. These concerns have manifested on a more regular basis in recent years with numerous revelations of companies covertly collecting personal data through various means and using that data for undisclosed purposes:

- In 2017, Bose Corporation was accused of secretly collecting and sharing personal information through its Bluetooth wireless headphones.[8]
- Vizio was recently forced to pay a $2 million settlement for collecting users' information without their knowledge, including tracking users' habits through their smart televisions.[9]

---

[6] Tim Johnson, *Why your next Echo command should be: "Disconnect me from the internet"* (May 8, 2017) Sacramento Bee, http://www.sacbee.com/news/nation-world/national/article148879664.html.
[7] Kevin Maney, *Meet Kevin Ashton, Father of the Internet of Things* (February 23, 2015) Newsweek http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html.
[8] Jeff Roberts, *These Popular Headphones Spy on Users, Lawsuit Says* (April 19, 2017) Fortune, http://fortune.com/2017/04/19/bose-headphones-privacy/.
[9] Hayley Tsukayama, *How to stop data collection on your Vizio (or other) television* (February 9, 2017) Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2017/02/09/how-to-stop-data-collection-on-your-vizio-or-other-smart-television/?noredirect=on&utm_term=.3495a88dd8f8.

- Earlier this month, it was revealed that a popular web-connected home security system found in many homes, Nest Secure, which is sold by a company owned by Google, contained a microphone that was not disclosed to consumers.[10]

The reach of data collection

Information is not just being collected from Internet-connected products. Consumers' Web browsing, online purchases, and involvement in loyalty programs also create a treasure trove of information on consumers. Many applications on the smartphones that most consumers carry with them throughout the day can track consumers' every movement.

This economy has given rise to the data broker industry, where the business model is built on amassing vast amounts of information through various public and private sources, and packaging it for other businesses to buy. A leader in this industry is Acxiom, a data broker that provides information on more than 700 million people culled from voter records, purchasing behavior, vehicle registration, and other sources.[11]

The collection of this data combined with advanced technologies and the use of sophisticated algorithms can create incredibly detailed and effective profiling and targeted marketing from this web of information. Acxiom offers "the World's Most Powerful Consumer Insights" with "comprehensive consumer data on approximately 250 million U.S. addressable consumers," or approximately 75 percent of the country's population.[12] The company provides a sketch of the data elements collected: individual demographics such as age, gender, ethnicity, education; number/ages of children; economic stability; marriage/divorce; birth of children; products bought; and behavioral details, including community involvement, causes, and gaming.

In response to this profiling, consumers have expressed growing concern. A study by the Pew Research Center found that 68 percent of American Internet users believe existing law does not go far enough to protect individual online privacy with only 24 percent believing current laws provide reasonable protections.[13] A recent study found that 74 percent of Facebook users did not know Facebook maintained a list of their interests and traits; 51 percent said they are not comfortable with Facebook compiling

---

[10] Richard Nieva, *Senate demands Google CEO answer for hidden Nest microphone* (February 27, 2019) CNET, https://www.cnet.com/news/senate-demands-google-ceo-answer-for-hidden-nest-microphone/.
[11] Nitasha Tiku, *Europe's New Privacy Law will Change the Web, and More* (March 19, 2018) Wired, https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/.
[12] *InfoBase®: The World's Most Powerful Consumer Insights*, Acxiom, https://www.acxiom.com/what-we-do/infobase/.
[13] Lee Rainie et al., *Anonymity, Privacy, and Security Online* (September 5, 2013) Pew Research Center, http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

this information; and 27 percent said the listings did not very accurately represent them, if at all.[14] The wave of revelations and scandals in recent years has likely only stoked the fears of consumers further.

There are also concerns that the intensive profiling of consumers can lead to socially detrimental outcomes. For instance, it was recently reported that anti-vaccination advocates have used Facebook's advertising platform "to target pregnant women with sponsored advertisements to spread false information and conspiracy theories as the U.S. battles a climbing measles outbreak." The advertisements have reportedly been viewed between one million and five million times. Arguably, this is an example of how such intricate profiling can go awry, abetting a systematic misinformation campaign in the middle of a growing health crisis. It is not hard to see how such processes could also radicalize individuals by exacerbating what could be a harmless first search or comment by then barraging the individual with content, products, and services that reinforces certain ideologies and behaviors.

Learning from Facebook

The Cambridge Analytica scandal most famously exposed the trove of data being collected by large businesses, the methods by which it is collected, and the potential for harm if that data is not properly protected.[15] Facebook offers a tool for software developers by which consumers can log into an app using their Facebook account rather than creating a new set of credentials; it is known as Facebook Login. However, this tool allows the app's developer to access a range of information on the consumer once logged in. In 2014, an app was created that 270,000 people logged into through Facebook Login. At the time, Facebook was also allowing these developers access to information about the friends of the consumer having so logged into the app. Through this branching access, the app and its creator were able to secure data from approximately 50 million consumers who had not given any consent to have their data harvested.

This data included information about consumers' locations, interests, photos, status updates, and more. This information was then funneled to a voter-profiling company called Cambridge Analytica. The explicit goal of the company and its financiers was to use personality profiling and psychographic messaging to shift broad scale culture and influence political battles. Such tactics endanger the very fabric of our democracy.

---

[14] Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data* (January 16, 2019) Pew Research Center, http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/.

[15] Matthew Rosenberg, et al., *How Trump Consultants Exploited the Facebook Data of Millions* (March 17, 2018) New York Times, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; Kurt Wagner, *Here's how Facebook allowed Cambridge Analytica to get data for 50 million users* (March 17, 2018) recode, https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

Despite the worldwide outrage in the wake of Cambridge Analytica and Facebook's role in it, there have been repeated incidents calling into question the social media company's data collection and retention practices. In September 2018, Facebook revealed that 30 million of its users were affected by a data breach. More alarming, half of those affected had particularly sensitive data stolen, separating it from other breaches. Facebook issued a press release indicating that 14 million users had a combination of the following information exposed: "username, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches."[16] Given the sensitivity of the data, it is argued that such a breach might be even more harmful than one stealing financial information: "Most data breaches involve financial information, but your Facebook account can be misused in a number of ways that are harmful. Accessing your private communications and posts by itself is pretty invasive, but that information could also be used to crack account security questions or to scam you and your friends."[17]

Already in 2019, two additional scandals have surfaced. The first involved the violation of Apple's terms of service through the use of "Facebook Research app":

> Desperate for data on its competitors, Facebook has been secretly paying people to install a "Facebook Research" VPN that lets the company suck in all of a user's phone and web activity, similar to Facebook's Onavo Protect app that Apple banned in June and that was removed in August. Facebook sidesteps the App Store and rewards teenagers and adults to download the Research app and give it root access to network traffic in what may be a violation of Apple policy so the social network can decrypt and analyze their phone activity, a TechCrunch investigation confirms.[18]

In just the past week, it was also revealed that a multitude of apps have been giving private data to Facebook without user's knowledge or consent.[19] One example is an app that allows women to track when they are getting their period and ovulation.

---

[16] Guy Rosen, *An Update on the Security Issue* (October 12, 2018) Facebook Newsroom, https://newsroom.fb.com/news/2018/10/update-on-security-issue/.

[17] Allen St. John, Here's What Makes the Facebook Data Breach so Harmful (October 12, 2018) Consumer Reports, https://www.consumerreports.org/digital-security/what-makes-the-facebook-data-breach-so-harmful/.

[18] Josh Constine, *Facebook pays teens to install VPN that spies on them* (January 2019) TechCrunch, https://techcrunch.com/2019/01/29/facebook-project-atlas/.

[19] Sam Schechner, *You Give Apps Sensitive Personal Information. Then They Tell Facebook* (February 22, 2019) Wall Street Journal, https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636; All Things Considered, *Apps Give Private Data To Facebook Without User's Knowledge or Permission* (February 27, 2019) NPR, https://www.npr.org/2019/02/27/698700499/apps-give-private-data-to-facebook-without-users-knowledge-or-permission.

Immediately upon uploading the information, the app sends the data to Facebook. Other information collected by these apps included weight, height, and blood pressure. What makes the covert collection of this extremely personal health information even more stunning is that there did not even need to be a connection to Facebook: "The social media giant collects intensely personal information from many popular smartphone apps just seconds after users enter it even if the user has no connection to Facebook." This is possible because the apps build in software from Facebook to enable various functions, such as tracking their users' behaviors. It is the software that sends the data back to Facebook regardless of whether the consumer is a Facebook user. The onslaught of such revelations have led to a rallying cry from consumers, privacy groups, and legislators across the country for stronger regulations to rein in what is being perceived as an assault on personal privacy.[20]

Surveillance Capitalism: A Framework for Understanding

Various frameworks have been asserted to understand the revolution in data collection and data deployment. One such framework has been posited by Shoshana Zuboff, an author and professor emerita of the Harvard Business School. She has coined the term "Surveillance Capitalism." She argues that the evolution of capitalism has always involved "claiming things that exist outside the market and bringing them into the market for sale and purchase." She argues: "Surveillance capitalism now claims private human experience as free raw material for translation into behavioral predictions that are bought and sold in a new kind of private marketplace. And it takes place almost completely without our knowledge."

As reported by Natasha Singer in the New York Times, this new sphere of the economy goes beyond digital advertisements:

> The technologies that power the behavior speculation market, of course, have spread far beyond online ads.
>
> They enable auto insurers to surveil drivers and offer discounts based on their driving performance. They allow workplace wellness programs to charge higher health insurance premiums to employees who decline to wear fitness trackers. They helped Kremlin-linked groups mount political influence campaigns on

---

[20] Bennett Cyphers & Jason Kelley, *What we should learn from "Facebook Research"* (January 31, 2019) Electronic Frontier Foundation, https://www.eff.org/deeplinks/2019/01/what-we-should-learn-facebook-research; Tony Romm, *Democrats vow Congress will 'assert itself' against tech – starting with Silicon Valley's privacy practices* (February 26, 2019) Washington Post, https://www.washingtonpost.com/technology/2019/02/26/democrats-vow-congress-will-assert-itself-against-tech-starting-with-silicon-valleys-privacy-practices/?utm_term=.fca70e7d17f1.

Facebook (although, as my colleague John Herrman pointed out this past week, we have yet to learn how effective those campaigns were).[21]

In a recent article in the Washington Post, Zuboff makes a call to consumers and elected officials alike that seems to echo the sentiments expressed decades ago by Assemblymember Cory and Senator Moscone:

> Surveillance capitalists soon discovered that they could use these data not only to know our behavior but also to shape it. This became an economic imperative. It was no longer enough to automate information flows *about* us; the goal became to *automate* us. As one data scientist explained it to me, "We can engineer the context around a particular behavior and force change that way. . . . We are learning how to write the music, and then we let the music make them dance."
>
> It works like this: Ads press teenagers on Friday nights to buy pimple cream, triggered by predictive analyses that show their social anxieties peaking as the weekend approaches. "Pokémon Go" players are herded to nearby bars, fast-food joints and shops that pay to play in its prediction markets, where "footfall" is the real-life equivalent of online clicks.
>
> This digitally informed behavior modification is carefully designed to bypass our awareness. It robs us of autonomy, of the freedom to choose our actions and of the right to say "no," eroding democracy from within. And it's a one-way mirror: These firms know everything about us, while their operations are unknowable to us. Their predictions are about us but not for us.
>
> Apple chief executive Tim Cook made this point recently while calling for a more comprehensive approach to privacy legislation: "Right now, all of these secondary markets for your information exist in a shadow economy that's largely unchecked — out of sight of consumers, regulators and lawmakers."
>
> Democracy has slept while surveillance capitalism has flourished. Elected officials determined to rein in the digital titans must understand that surveillance capitalism is bigger than any single company. Regulation will require a new framework that strengthens our understanding of privacy rights. We will need to interrupt and in some cases outlaw (1) the unilateral claim to private human experience as a free source of raw material and its translation into data; (2) the exclusive concentrations of knowledge illegitimately gleaned from our behavior; (3) the manufacture of computational prediction products based on the secret capture of our experience; and (4) the sale of behavioral prediction products.

---

[21] Natasha Singer, *The Week in Tech: How Google and Facebook Spawned Surveillance Capitalism* (January 18, 2019) New York Times, https://www.nytimes.com/2019/01/18/technology/google-facebook-surveillance-capitalism.html.

Our democracy has successfully confronted many excesses of unchecked capitalism, outlawing child labor, uninspected food and unfair wages. Today we face a similar challenge in curbing the excesses of a rogue surveillance capitalism. It is not the work of a day or a year, but it is necessary work, and we must be up to the task, because the alternative promises dangerous consequences for human freedom and democracy.[22]

[22] Shoshanna Zuboff, *'Surveillance capitalism' has gone rogue. We must curb its excesses.* (January 24, 2019) Washington Post, https://www.washingtonpost.com/opinions/surveillance-capitalism-has-gone-rogue-we-must-curb-its-excesses/2019/01/24/be463f48-1ffa-11e9-9145-3f74070bbdb9_story.html?utm_term=.2ec9dac6f90f.