What did the digital age mean for privacy in the United States?

Achyuth Rachur
Jonathan Putman
Clifford Fisher
Purdue University, USA

Keywords
Cambridge Analytica, Data Privacy, GDPR, privacy

Abstract

Over the course of the last 3 decades, the world has seen monumental shifts in how information is collected, transmitted, and disseminated. Every aspect of our personalities that live on the internet, including our browser history, photos we post to social media, our shopping decisions and our selection of online friends, has been collated, quantified, and assimilated into a digital profile, which has skyrocketing value to an increasing number of businesses. With these developments in technology come the inevitable questions of ownership of such data, its use, misuse and even possible theft. This paper takes a comprehensive and comparative look at the data privacy legislature in the two largest data hubs in the world, namely the United States and the European Union. The paper also seeks to address the shortcomings of certain, past legislative decisions, and makes a recommendation for the future. To do this, we analyze the events of the past, using the 2016 Facebook/Cambridge Analytica data scandal as a focal

point. On analyzing the major differences between American privacy law and the preeminent document on data privacy at the time, namely the Global Data Privacy Regulations (GDPR), we conclude that data privacy in the United States is in its nascent stages, in dire need of an overhaul. The California Consumer Privacy Act is the legislature that comes close to mimicking the function of the GDPR, albeit at a much smaller scale. The other remedies include the American Data Privacy and Protection Act (ADPPA), which is already under consideration by Congress, or a state-by-state approach.

Corresponding author: Achyuth Rachur
Email addresses for the corresponding author: arachur@purdue.edu
The first submission received: 15th June 2022
Revised submission received: 10th September 2022
Accepted: 15th October 2022

Introduction

With legally challenging privacy questions arising frequently in major news headlines and the judiciary system of the United States, it becomes routine for the public to find subjectively easy answers to objectively hard cases. However, there is nothing simple about drawing lines around privacy. In the volatile age of ransomware, government surveillance, and big data two things remain true. First, Americans feel unprotected and out of control when it comes to their personal data and online privacy. Research conducted by Pew found that 81% of U.S. adults say that "they have very little or no control over the data that… companies collect about them," yet these results do not end here (Auxier et al. 2019). Pew also found that a similar percent of Americans are concerned with the risk of their data being collected, the lack of control of their data, and the tracking of their actions online (Auxier et al. 2019). While Pew research has also found that 75% of U.S. adults believe there should be more government regulation protecting consumer data, our second truth highlights legal privacy is in constant flux (Auxier et al. 2019).

Throughout history it has been held that the magnitude of rights expands and contracts according to the will of the people and those in power. In one of the earliest writings on American privacy, future Supreme Court Justice Louis Brandeis stated that the "development of law was inevitable" (Warren et al. 1890). In accordance with Brandeis statement, the law is never static; instead, it is constantly in a tug of war between parties with different agendas. The question with privacy is not whether it is in a state of contention, but rather if the necessary policy change to pull privacy in the favor of the individual will be implemented in time. However, before a discussion on the future of privacy in the United States can occur

it is necessary to understand the current judicial and legislative position on privacy and the critical cases that established the principle.

Background

Data Privacy in the Courts

Griswold v. Connecticut, 381 U.S. 479 (1965) was the landmark decision in which the Supreme Court found that the right to privacy is established from penumbras found in the Bill of Rights. The Court rules that there existed a "zone of privacy" created by the inferred Right to Privacy, and an individual could not be forced to release this by the government. *Katz v. United States*, 389 U.S. 347 (1967) furthered the right to privacy by extending the interpretation of the Fourth Amendment to "protect people, not places." A bound to these privacy rights is found in *Whalen v. Roe*, 429 U.S. 589 (1977). It was here that the Supreme Court found that collecting and storing sensitive patient information is not a violation of privacy covered by the Fourteenth Amendment. It was also found that the doctor-patient relationship is not within the zone of privacy.

The following cases document a relatively new extension of privacy litigation that focuses on the unconstitutional procurement of data. The concept of the "third party doctrine" is established by *United States v. Miller*, 425 US 435 (1976). Under this reasoning, an individual should not "reasonably expect privacy in information they willingly disclose to third parties." *Kyllo v. United States,* 533 US 27 (2001) found that technological searches of a home, by the government, are unconstitutional under the 4th amendment when the device is not in "general public use." This finding was to protect individuals from "the mercy of advancing technology." In *Carpenter v. United States*, 585 U.S. ____ (2018) it was held that the warrantless seizure of Timothy Carpenter's cell-site evidence violated his Fourth Amendment right against search and seizure. Carpenter simultaneously restricts the power of the "third-party doctrine" by deciding that simply because data is "held by a third party does not by itself overcome the user's claim to" protections under the Fourth Amendment, but instead these protections must voluntarily be reduced.

This very simple history is aimed to prepare the reader for the complex and contrasting nature of privacy within the federal courts. As shown in the examples above, the courts have longstanding legal precedents that did not envision the technological privacy battles that are currently making front pages. This forces the courts to find creative rulings from outdated provisions and tests that do not always put the protection of the people at the center of the decisions.

Data Privacy in the Legislatures

Legislatures across the globe have voiced growing concerns over citizens' rights to control their own personal data. These concerns give rise to a multitude of questions: Is an individual's personal data considered that individual's property? If so, should individuals required to be compensated when their data is used for the economic gain of a third party? Do individuals maintain ownership of their data when personal information is used without their knowledge? Are individuals allowed to demand their data be erased from databanks or archives at their discretion? (What is personal data?, 2022)

It is not easy to answer these questions under the purview of existing legislation to form a map to what future legal framework concerning the privacy of citizens on the internet must enshrine. Indeed, this is a complex question based in technology that evolves multitude faster than any law that is passed to protect those individuals. However, there are foundational principles that can guide the discussion.

In a seminal article on the right to privacy written in 1890, future Supreme Court Justice Louis D. Brandeis put it this way: "The common law secures, to each individual, the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others." In the next 100 years, the concept grew to include, "[t]he right to informational privacy is succinctly defined as the right of the individual to maintain control over personal information concerning one's 'physical and individual characteristics, knowledge, capabilities, beliefs and opinions." Because of that principle, it is a natural extension to say that an individual also has a right to claim certain rights. Specifically, privacy is the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

Perhaps the most fundamental question to ask remains one of property rights: is data property at all? While there is no comprehensive federal law related to data privacy in the United States, we can look to the European Union's General Data Protection Regulations (GDPR) for potential guidance. Article 4, Clause 1 of GDPR defines data 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'

Classifying an individual's personal data has multiple positive ramifications. Personal data includes data to which they have a reasonable expectation of privacy, such as their preferences on various aspects of their life such as religion and sexuality, information regarding ethnicity on online employment applications, and conversations that may be had over the internet (for example, via a text messaging service or a social media network like Instagram). This may even extend to more confidential information like credit card numbers, as an individual's personal property. Perhaps the most significant of these is the well-established right of an individual over personal property, an institution of thought that began with jurists like Bartolus of Sassoferatto, who wrote in the fourteenth century. Bartolus defined property (dominium) as the "right of complete control over a physical object, to the extent not prohibited by law" (*ius de re corporali perfecte dispnonendi nisi lege prohibeatur)*. This very definition was later expanded by Bartolus himself, into one that has widespread implications in today's world. Property, he said, "may be used to refer in the broadest sense to every incorporeal right, as in 'I have property in an obligation, for example in a usufruct'" (*potest appellari largissime pro omni iure incorporali, ut habeo dominium obligationis, utputa usufructus).*[1] This establishes a natural right of privacy over an individual's personal property (in this case, personal data). Most notably this has been expanded in "The Right to Privacy" by Warren and Brandeis in the Harvard Law Review in 1890, as the "right to be let alone," arguing that "the principle which protects personal writings and any other productions of? the intellect or the emotions, is the right to privacy."

What modern technology has created is a situation where the law is forever behind the bounds of technology. In practice this means that the definitions of privacy and property are not matched with the actual way we articulate and use them. The challenge has been expanding definitions of property into currently existing frameworks, to accommodate data and what it includes. All it takes is one data breach to remind each of us how important these protections and their lack impact each of us.

Is Data Property?

Before we can fully address whether there is a privacy right in an individual's data, we should first examine whether data is property. That requires a clear understanding of what we mean by data.

Data takes multiple forms, some classified as general facts or information. Data generally has no restrictions imposed that defend individuals regarding collection and publication of data. However, the data that concerns one's "physical and individual characteristics, knowledge, capabilities, beliefs and opinions" as in *Downing v. Municipal Court of San Francisco* that is of note here. The word 'property' has been the subject of innumerable definitions, and in *Downing*, the court took the position that "the word property is all embracing, so as to include every intangible benefit and prerogative susceptible of possession or disposition".This interpretation of property was expanded in *Kremer v. Cohen,* where the Ninth Circuit applied a three-part test regarding the existence of property rights. "First, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity." Data meets this test because it has a precise definition (See the GDPR definition above). It is also exclusively controlled by the

owner with a license to those the data is given, sold, or shared with. And finally, personal data is personal by its very nature. It is owned by the person the data describes unless an alternative agreement is reached. As a property I own, I can sell it to someone if I decide it is valuable. The corollary is that I continue to own that data unless I choose to sell or license it to someone.

Because data is property, the rights that define property are then naturally extended to data, including the right to "use it as one wishes, to sell it, give it away, leave it idle or destroy it". These rights tend to entail the following:

The Right to Use as One Wishes

When personal data (ie. the data used to identify an individual on the internet, also called a digital fingerprint) is communicated to a third party, the user/owner has a reasonable expectation that the third party will keep said data confidential. It is more interesting to look at the expectation that the law has of the third party. "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." The law has also upheld that the provision of personal data to a third party does not transfer the ownership of the data from the user to said third party, as evidenced by the Ninth Circuit's ruling in *HiQ Labs v. LinkedIn,* wherein the appellate court held that the members had a privacy interest in their data that LinkedIn had to protect. The court stated that "LinkedIn has no protected property interest in the data contributed by its users, as the users retain ownership of their profiles."

While the United States doesn't have a broad data privacy law, we can look to California and European Union laws for some guidance on how the federal government could structure a law that clarifies the rights individuals have to control the use of their personal data. First, the CCPA Right to Opt-Out law gives consumers in California limited rights against data selling businesses. Specifically, it affords consumers the "right to, at any time, direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out." Under the GDPR, consumers have expanded rights that include the right to be forgotten. This regulation provides that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay. . ."

The Right to Sell

If we can reasonably assume that an individual has the right to sell property and this right extends to personal data, this brings into question the concept of assigning value to an individual's personal data. It also brings into consideration who decides the value and, the parameters that are used to arrive at said value. Another concept of note is how prospective damages are to be calculated, in the case of theft of an individual's personal data.

The Right to Give Away

A corollary to the right to sell is the Right to Give Away, or transfer, one's personal data. This may be the area of property law where arguably the largest differences exist between tangible physical property and intangible personal data. The concept of transferability states that property can be "assigned, sold, transferred, conveyed or pledged", leading to the natural conclusion that that which cannot be transferred is not property. In the matter of intangibles, the concept of 'transferability' has been interpreted to apply to a relinquishment of the owner's rights to said property, which could allow others to use data whose use may have been restricted by a right to privacy. This principle runs into obstacles when taken in context of recent data privacy and regulation legislature, such as the CCPA and the GDPR. The wording of the laws and regulations are an indication of the intent that a data subject cannot relinquish their rights over personally identifiable information (PII) in their entirety. Instead, they many license to the business the right to use that data for certain purposes, such as when Netflix uses your geographic location to recommend a movie that is trending in your country, or Amazon uses your location to alert you that a product that may not reach your address within a stipulated timeframe. However, these restrictions do

not circumvent the classification of data as property, even if certain rights are restricted or precluded by specific legislature in select jurisdictions.

The Right to Destroy

Does an owner have a right to tell a third party to destroy that individual's data that has been mined and collected by the third party? Without this key property right, can data truly be owned by the person the data is created by or used to describe? If I own my home, I can destroy it for any or no reason so long as insurance fraud or other harm is not conferred on another person or company. I can do the same with my personal property. However, the right for me to destroy or order a third party to destroy my data is difficult to enforce. That difficulty does not preclude my ownership of that data.

Data Protection Principles found in the United Kingdom's Data Protection Act, the British implementation of the European GDPR, can be helpful in providing a framework for the obligations a third party has to protect individual's data that it either collects or is entrusted with for any reason. This act states the following:

Everyone responsible for using personal data must follow strict rules called 'data protection principles.' They must make sure the collected information is:
Used fairly, lawfully, and transparently
Used for specified, explicit purposes
Used in a way that is adequate, relevant, and limited to only what is necessary
Accurate and, where necessary, kept up to date
Kept for no longer than necessary and
Handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction, or damage

There is stronger legal protection for more sensitive information, such as information related to race, ethnic background, political opinions, religious beliefs, trace union membership, genetics, biometrics, health, sex, and sexual orientation.

Under the Data Protection Act of 2018, you have the right to find out what information the government and other organizations store about you. These include the right to: be informed about how your data is being used, access personal data, have incorrect data updated, have data erased, stop, or restrict the processing of your data, data portability, and object to how your data is processed in certain circumstances.

The United States operates on a primarily sectoral approach, with data privacy legislation being implemented on an ad hoc basis. This allows different sectors, such as those of healthcare, financial services, and education to have separate, tailored data privacy laws. These include the Health Insurance Portability and Accountability Act (HIPPA), Genetic Information Nondiscrimination Act (GINA), Gramm Leach Bliley Act, and Family Educational Rights and Privacy Act (FERPA) to name a few. The challenge in the United States then stems from the lack of a unified federal data protection law, to regulate the protection of personal, identifiable data, and represents what is arguably the biggest flaw in the United States' approach toward an individual's right to privacy and ownership over personal data on the internet.

What was the Facebook/Cambridge Analytica Data Scandal?

In March 2018, David Carroll, a professor at the Parsons School of Design in New York filed a legal challenge in Britain, requesting the court to require Cambridge Analytica to disclose the alleged '5000 data points' that it had on every American Voter. The filing of the challenge reverberated across the world, and the crowdfunded case became an international spectacle in part thanks to the Netflix documentary *the Great Hack*. However, the roots of the scandal are much deeper and broader than one man or one documentary. The scandal has become well known for shining a scathing light on the commercial advertising-technology marketplace that utilizes innumerable data mining techniques to track, identify, and specifically target users across the internet and online platforms. Facebook banned Cambridge Analytica from the network, in a too little, too late effort, claiming Cambridge had siphoned the personal information of over 87 million Facebook users and had failed to delete the same as requested.

The Cambridge Analytica scandal created global shockwaves for a multitude of reasons, some well-known, such as the stark lack of privacy that a user of the popular social media network Facebook could expect, or the sheer volume of users (approximately 50-65 million according to Ingram, 2018) who had data mined, processed, and misappropriated. While some reasons are not as well known, one of them is the nascent stages that American Federal Data Protection legislature was in when compared to that of the European Union or the United Kingdom.

Why does this matter? The Facebook/Cambridge Analytica data breach has been alleged to have contributed to Trump winning the presidency in 2016. Beginning in 2013, Aleksandr Kogan, a professor, and data researcher at Cambridge University, developed an application for a personality quiz, named "This is Your Digital Life". The application would appear on the social media network, Facebook in 2014, and claimed to its users that the "results of the quiz would be used for academic purposes". Approximately 270,000 people consented to divulging personal data, and data about their Facebook friends, which was permitted at the time under Facebook's policies (subject to user's individual privacy settings). Most didn't realize they were divulging access to their personal data stored on the app as well as giving access to their friends' data, although that was included in the terms and conditions of using the quiz.

An article in *The Guardian* in December 2015 alleged that Kogen sold confidential information mined through the "This is Your Digital Life" app to Cambridge Analytica through his company Global Science Research. This was a clear violation of Facebook's policies. In the weeks and months that followed, Cambridge Analytica developed psychological profiles for tens of millions of US voters to support Ted Cruz's presidential campaign, using the data sold to them by Kogan. Following the publishing of the article, Facebook removed the application from its site and privately asked GSR and Cambridge Analytica to delete the data stored about the users and was assured that the pertinent information had been deleted. However, Facebook did not take steps to confirm this. Three years later, stories published by the *New York Times* and *The Guardian* alleged that the Cambridge Analytics lied when it said the data had been deleted and instead had used it in connection with President Donald Trump's campaign. Cambridge Analytica, its parent company, and relevant employees were suspended from the Facebook Platform.

These revelations resulted in three major legal actions, which have three different perspectives to the current state of data privacy legislature within the United States. First, David Carroll's formal legal claim against Cambridge Analytica's parent company, SCL, through a UK based human rights lawyer, on the advice of Swiss research specialist and the founder of a digital rights non-profit, Paul-Olivier Dehaye. Carroll's claim was pursuant to the provisions of the UK's Data Protection Act of 2018, which states that a data subject has the right to access personal data that was being processed or stored by the government or a company. Approximately a month later, Carroll was served with a response to his claim, which consisted of information including his opinion on issues like national debt, immigration, and gun rights; however, the information was nowhere near the 5000 data points that Cambridge Analytica claimed to have on every American voter through the data it had collected. As the movement gained international attention and Carroll pursued legal action against the company, his data was never turned over to him. Over the course of the next two years however, the involvement of the UK Information Commissioner's Office and the FBI proved to be a significant catalyst to expedite the process. By providing Carroll with a portion of his information, SCL had agreed that the UK's Data Protection Act applied to non-British citizens, if the data was processed within the UK, as Cambridge Analytica did. In addition, by refusing to provide Carroll with the data in its entirety, SCL violated the Act and was liable.

As of January 2020, Carroll was quoted saying "I haven't had my data back yet. We are awaiting the report from the UK Information Commissioner's Office, the organization responsible for regulating these matters. It is a process in which we may have to wait for notifications from the FBI and the British parliament" (Fischer, 2019). The GDPR has made considerable strides on the data protection front, and "applies to the processing of personal data of data subjects who are in the Union by a controller, or a processor not established in the Union". The CCPA is the first step in the right direction for a US law but only applies in California. The lack of a federal law regarding data privacy leads to several gray areas, with little to no consistency on the rules with which organizations must comply.

A second lawsuit involved the Facebook Inc. Securities Litigation. The lawsuit was filed by purchasers of Facebook common stock between 3rd February 2017 and 25th July 2018, alleging that Mark Zuckerberg, Sheryl Sandberg, and David M. Wehner deliberately misled investors about the course of dealings with Cambridge Analytica, in violation of Section 10(b), 20(a) and 20A of the Securities Exchange Act. The suit further argues the investors were led to believe that omissions "concerning Facebook's privacy and data privacy practices" would not have a negative implication on Facebook's stock prices during the time periods of March and July 2018. A third lawsuit complemented the securities lawsuit. In the Facebook Inc. Consumer Privacy User Profile Litigation, an action by social media users against Facebook, the plaintiffs alleged Facebook shared the user's personal information with third parties when Facebook did not have a right to share the information. Facebook filed a barrage of motions to dismiss, some of which were accepted by the court.

In both lawsuits, the court held that Facebook had no obligation to confirm the deletion of data by Cambridge Analytica and SCL, since nowhere in Facebook's data policy was there a representation that Facebook would confirm deletion. Instead, the policy only represents that Facebook would "require data to be deleted", with no guarantees about how Facebook would enforce that requirement.

This judicial ruling highlights the need for federal legislation regarding data privacy, storage, processing, etc. This is especially relevant as one seeks to draw parallels between the offenses that Facebook was found guilty for in the US, and the policies that it would have been found to be in contravention under the GDPR. A fairly well-established provision of the GDPR under Article 17 is the Right to Erasure of the Right to be Forgotten. Clauses (1) and (2) state that when a data subject has made a request of erasure of personal data concerning them, the controller shall have the obligation to erase said personal data without undue delay, taking account of available technology and cost of implementation, taking reasonable steps to accomplish the same. On the surface, this seems to be fairly in line with Facebook's data policy concerning deletion. What sets the GDPR and the UK Data Protection Act of 2018 as a higher standard is the clear definition of penalties to be imposed is requests are not reasonably complied with. Article 77 grants a data subject the right to lodge a complaint with a supervisory authority, in the member state of their habitual residence, detailing the alleged infringement committed, following which they are to be kept updated on the progress or the outcome of the complaint, which may result in fines (to be established by the relevant member state) (Article 83 & 84), judicial action agains the defendant (Article 78 & 79), and the right to compensation for the plaintiff (Article 82). In the case of Cambridge Analytica, the UK's Information Commissioner's Office issued an order directing the firm to supply Carroll with his data within thirty days, failure to comply with which would result in criminal charges.

The fourth action occurred at the Federal Trade Commission (FTC). The FTC found Cambridge Analytica liable on multiple counts, including its practices concerning the collection of Personally Identifiable Information, its claims regarding its participation in Privacy Shield - a framework designed by the US Department of Commerce, the European Commission, and the Swiss Administration in order to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU and Switzerland to the United States in support of transatlantic commerce - and the subsequent adherence to the provisions of the framework. The first count, that of misrepresentation, arose out of a statement that anyone who downloaded the Cambridge Analytica survey on Facebook would see, which stated that, "In this part, we would like to download some of your Facebook data using our Facebook app. We want you to know that we will NOT download your name or any other identifiable information—we are interested in your demographics and likes." The court found the statement was misleading, following evidence that the company had in fact harvested, downloaded, and misappropriated the user's PII. The counts regarding the Privacy Shield framework and the subsequent compliance with its principles, stemmed from the fact that Cambridge Analytica did not renew their certification of compliance with the Privacy Shield, and therefore was in contravention of the policies codified by the framework. The lawsuit, although monumental, and may set precedent for the future, was born out of the lack of a federally regulated data privacy and protection statute and is one of the most indicative signs that the United States has fallen behind the EU and the

United Kingdom in this aspect, and a federally regulated statute would serve as the broadest possible authority with regard to data privacy, as opposed to the currently used ad hoc patchwork system.

Why isn't everything Data Misappropriation?

In many large cases with claims of data misuse and misappropriation, it is easy for an individual to find the accused party guilty at first examination, but quick glances are not always accurate. In 2009 the American Recovery and Reinvestment Act gave the Department of Energy the ability to provide funds to cities through the Smart Grid Investment Grant program with the goal of modernizing the nation's energy grid. Naperville, Illinois was one of the cities selected under this grant program to receive $11 million to modernize their own grid (*Naperville Smart Meter Awareness v. City of Naperville* 2018). In this modernization, Naperville replaced their old energy meters with "smart meters." The traditional meters would measure monthly "energy consumption in a single lump figure once per month," but the new smart meters recorded energy consumption data in "fifteen-minute intervals." Because of distinct "load signatures" exhibited by appliances in these data measures, it can be predicted with great accuracy what appliances are in each home and at what times they are being used. Upon learning about this perceived breach of privacy, a group of citizens whose homes were now using the new smart meters created Naperville Smart Meter Awareness to bring suit to the program. Their argument alleged that the smart meter system implemented by the City of Naperville was a direct breach of the Fourth Amendment and was therefore an unlawful search and seizure of data. The United States Seventh Circuit Court looked at the following two questions to measure the validity of the plaintiffs claim. First, is the data collection in this case truly a search? Second, was the search unreasonable as stated in the Fourth Amendment?

For the first question, the court looked specifically to the previous mentioned case *Kyllo v. United States* [2001] 533 U.S. 27. In *Kyllo* the Supreme Court ruled that when sophisticated technology provides information that would be "unknowable without physical intrusion, the surveillance is a 'search.'" As mentioned by Smart Meter Awareness, the collection of data through the smart meters provides extreme personal data and routines that would not be accessible without a physical search. The court also notes that in *Kyllo* the 'search' was via thermal imaging tools and provided more crude data than the constant stream of 15-minute datapoints collected by Naperville. From these arguments the court found that the non-voluntary implementation of smart meters was indeed a 'search' of the residents' homes. However, the court still had to decide if the collection of this data met the Fourth Amendment requirement of being unreasonable?

For this second question, the court mainly points to the precedent of *Camara v. Municipal Court* [1967] 387 U.S. 523. to examine the reasonableness of the search. While the court finds the smart meter's collection of data to be a warrantless search, the court also must consider that the City of Naperville had "no prosecutorial intent" when committing the search. In *Camara* the Supreme Court takes note of this intent and states that it "is a less hostile intrusion" since it is not to find criminal evidence, which allowed the court to examine fewer protections and only focus on the "right to be secure from intrusion into personal privacy." While this situation is like Naperville, the court found that the threat posed by smart meters is not as high as the situation threats in *Camara*, like lack of physical entry into the homes and the diminished chance of situational prosecution. These distinct differences in relative chance of prosecution separated the two cases from receiving the same outcome. The court also explained the need to weight privacy concerns against the "government interest in data collection." In this situation the court held that the role smart meters play in the modernization of the electrical grid is high enough to warrant the collection of data from the public. Because of these two reasons, the court ruled that the warrantless 'search' of property through the smart meters was not unreasonable because it served a genuine government interest without being unreasonably intrusive. However, the court mentions that this ruling is a narrow one and that if minor details of this case were changed, the ruling would change with it. Nevertheless, this case shows that there are many situations in which, at a first glance warrantless searches through innovational technologies look unreasonable yet are found reasonable through the review of the courts. Narrow rulings, such as *Naperville Smart Meter Awareness v. City of Naperville,* play a large role in the general, undefined, and murky world of tech privacy in the United States.

Discussion: What does the future hold?

Data privacy is a complicated and cutting-edge issue that has been thrust further into focus by recent cases like Cambridge Analytic. The United States is currently tasked with developing a rigorous legislative backbone that defends individuals' data across the nation. Building on the regulatory successes of the GDPR in Europe and the CCPA in California, two logical regulatory approaches arise.

Congressional Legislation

The United States could create federal legislative policy that promotes and protects data privacy in a top-down approach. This style of regulation is already underway in Congress under the title of the American Data Privacy and Protection Act (ADPPA). Following very closely to the groundwork set by the GDPR, the ADPPA outlines consumer data rights and corporate accountability measurements to create regulation protecting consumer data under the authority of the Federal Trade Commission (FTC). The ADPPA would cover the lack of a unified federal data protection legislature, which is undoubtedly data privacy's biggest weakness in the United States. It is what leads to the current sectoral approach, which allows independent industries to draft and enforce data privacy legislature, with little to no uniformity leading to contradictory and overlapping protection for citizens. However, there is another opportunity for privacy reform in the United States.

Code Regulation

If the ADPPA becomes stalled and does not pass via Congress, another opportunity to create nationwide regulation comes from enacting a code on the State Legislative level. Like the regulatory code of the UCC, the United States could hire independent experts from institutions, such as the American Law Institute, to develop a set of regulatory codes for data privacy. This set of regulatory code would then be given to every state legislature to make individual revisions to and ultimate vote into law. While there is always the risk that multiple states could reject the code created by this body, there are many strengths found from this model. Under this system, every state would be able to implement regulatory laws that protect their citizens in a broad and definitive manner, but also allow for freedom to individual expand the regulations as data becomes more complex. This adaptability allows for data regulation to continually change with new problems, instead of remaining dormant by a gridlocked Congress or other pressing federal matters. The individual changes of the states would also create a regulatory umbrella

California is perhaps the closest replicable example for the American legislators, as the CCPA enshrines some of the strictest data privacy laws ever seen in the United States. It is not only significant for the fact that it required identical controller/processor requirements to the GDPR, but for the way it views an individual's right to data privacy. Just as the EU regards data privacy as a fundamental human right and seeks the build the provisions of the GDPR around that central right, the California Constitution views "privacy" as an inalienable right, not to be limited by other rights.

Whether the United States' data privacy regulation is formed through congressional legislation or regulatory codes is of minor importance when compared to the necessity of any form of regulation.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. and Turner, E., (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. [online] pewresearch.org. Available at: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (Accessed 17 February 2022).

Warren, S. and Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5), pp.193—197 (Accessed 2 August 2022).

European Commission - European Commission. (2022) *What is personal data?*. [online] Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (Accessed 8 August 2022)

Griswold v. Connecticut (1965) 381 U.S. 479 (Accessed 3 July 2022).

Katz v. United States (1967) 389 U.S. 347 (Accessed 8 July 2022).

Whalen v. Roe (1977) 429 U.S. 589 (Accessed 29 April 2022).

United States v. Miller (1976) 425 U.S. 435 (Accessed 29 April 2022).

Kyllo v. United States (2001) 533 U.S. 27 (Accessed 29 April 2022).

Carpenter v. United States (2018) 138 S. Ct. 2206 (Accessed 29 April 2022).

Grossman, E. (1986). Conceptualizing National Identification: Informational Privacy Rights Protected. *UIC Law Review*, 29(4), pp.5. Available at: https://repository.law.uic.edu/lawreview/vol29/iss4/15/ (Accessed 13 March 2022)

Austin, L. (2018). Re-Reading Westin. *Theoretical Inquiries in Law, Forthcoming,* 20(1), pp.5 (Accessed 6 August 2022).

Regulation (EU) (2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)'. (2016). *Official Journal,* L 119, pp.1-88. Available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

(Accessed 4 June 2022)

Boyce, B. (2007). Property as a Natural Right and as a Conventional Right in Constitutional Law. *Loyola of Los Angeles International and Comparative Law Review*, 29(2), pp.16 (Accessed 21 July 2022).

Downing v. Municipal Court of San Francisco [1948] 88 Cal. App. 2d 345 (Accessed 29 April 2022).

Kremen v. Cohen (2003) 337 F.3d 1024 (Accessed 29 April 2022).

Phoenix, J. (2021). *What is a Digital Fingerprint?*. [online] Available at:

https://understandingdata.com/what-is-a-digital-fingerprint/ (Accessed 23 February 2022)

HiQ Labs, Inc. v. LinkedIn Corp. (2019) 938 F.3d 985 (Accessed 31 January 2022).

California Legislature, (2020). CIV. § 1798.120(a) (Accessed 10 June 2022).

In Re Marriage of Graham (1978) 574 P.2d 75.

Ingram, M. (2018). *'It just felt right': David Carroll on suing Cambridge Analytica.* [online] Available at:

https://www.cjr.org/q_and_a/lawsuit-cambridge-analytica.php

Data protection. [online] Available at: https://www.gov.uk/data-protection (Accessed 27 May 2022)

Federal Trade Commission *(2019) UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION In the Matter of Cambridge Analytica, LLC, a corporation. Docket NO. 9383. Available at:*

https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opini onpublic.pdf (Accessed 18 July 2022)

In re Facebook, Inc. Sec. Litig. [2020] 477 F. Supp. 3d 980 (Accessed 31 March 2022).

Lapowsky, I. (2019). *One Man's Obsessive Fight to Reclaim His Cambridge Analytica Data*. [online] Available at:

https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/ (Accessed 1 March 2022)

United States International Trade Administration. *Privacy Shield Program Overview*. [online] Available at:

https://www.privacyshield.gov/program-overview (Accessed 28 July 2022)

Whalen v. Roe (1977) 429 U.S. 589 (Accessed 28 March 2022).

Naperville Smart Meter Awareness v. City of Naperville) [2018] 900 F.3d 521 (Accessed 13 March 2022)

Fischer, W., (2022). *We talked to the professor who fought Cambridge Analytica to get his data back in Netflix's 'The Great Hack' about why privacy rights in the US are lagging behind the rest of the world*. [online] Business Insider. Available at: https://www.businessinsider.in/tech/we-talked-to-the-professor-who-fought-cambridge-analytica-to-get-his-data-back-in-netflixs-the-great-hack-about-why-privacy-rights-in-the-us-are-lagging-behind-the-rest-of-the-world/articleshow/70726124.cms (Accessed 1 August 2022).