Connecting the World: Privacy Violations and the Harm Principle in the Facebook-Cambridge Analytica scandal

by

Rick van der Veer

Dr. M.G. Valenta

MA Thesis North American Studies

August 25, 2019

Abstract

In the spring of 2018, the data company Cambridge Analytica was accused of having leaked and abused the Facebook user data of tens of millions of people against their will. This data was used to influence elections around the world, including the United States and the United Kingdom. In order to determine if users were harmed by this data leak, John Stuart Mill's harm principle can serve as a threshold determination, but it must be placed in the proper context in order to do so. The Facebook scandal needs to be positioned in the history of privacy in the United States to determine its place in the debate, how Facebook is dealing with the subject, and what predictions can be made for the future. Furthermore, the future of social studies must be considered in the context of using user data from Facebook, as issues with research data from this social network have occurred several times in the past.

Keywords: harm principle, John Stuart Mill, Cambridge Analytica, Facebook, privacy

Acknowledgements

I would like to thank my supervisor dr. Markha Valenta for her enduring support during the thesis trajectory, even though getting to the finish line took me longer than most other students. I would also like to thank dr. Jorrit van den Berk, who graciously agreed to act as second reader for this thesis.

In addition, I would like to express a great deal of appreciation to Iris Monteiro for the deep conversations about studying, sports, and what it means to overcome one's own limitations in the process of writing a master's thesis.

Last but not least, my deepest appreciation goes out to Julia Helsloot, for keeping me sane during the writing process.

Table of Contents

Introduction

In the twenty-first century, social media has become a part of life that nearly everyone is a participant in, in one way or another. Many people use Facebook or Twitter to post updates on their personal life or share pictures through Instagram or Snapchat. In many countries, messaging apps such as WhatsApp have replaced more traditional forms of communication, such as text messaging or phone calls. Even those who choose not to use social media to share personal data might still use websites such as LinkedIn to maintain a professional network or to find jobs that match their skillset. Many other online activities, such as playing video games, have also incorporated their own way of interacting with other users, in the same spirit as other social media. Even businesses and corporations have resorted to social media-like applications to provide tools for communication, such as internal chat channels, customer service chats, or social media platforms for internal use. In other words: mankind is more connected in the digital realm than ever before.

The result of these developments is that a handful of corporations have become stewards of a wealth of personal data. Facebook is not only the owner of its namesake social network, it also operates Instagram and WhatsApp, the latter of which is arguably the de facto standard in text messaging in many countries. This messaging app, allowing users to send messages, pictures, and videos to others, grew from 200 million users in April 2013 to over 1.5 billion users worldwide in December 2017 (Constine). That number has only gone up since then.

In 2014, a data company called Cambridge Analytica used a Facebook app to collect survey data from a group of thousands of Facebook users. That data was supposedly meant to be used for academic research but collected much more than what was originally the intent. When a Facebook user consented to the usage of their profile data for that app, their friends' data also

became accessible. Through this unintentional method, up to 87 million profiles were accessible and subsequently harvested for data deemed interesting (Cadwalladr and Graham-Harrison). Facebook later changed the amount of information apps can access and limited the scope of data collection to just a user's own profile, but at the time, the app had access to hundreds of thousands of profiles

To establish what happened with Cambridge Analytica as a proper case study, the relevant facts must be accounted for. Following the incident, many news outlets published on the story, leading to a fragmented narrative of what the relevant facts were. Several prominent journalists took an interest in the story and made it their primary focus, which means that their work is well-researched. Especially the British news outlet *The Guardian* has made it one of their priorities to provide independent and accurate reporting on the matter. Along with the *New York Times*, they were one of the first sources to publish on the incident. For this reason, *The Guardian* is one of the primary sources of information for this thesis regarding the facts of the matter.

The first time Cambridge Analytica received any kind of prominent media attention, was in December of 2015, when *The Guardian* broke news that the Republican presidential candidate Ted Cruz had used a data company to boost his White House run. This company had gathered "psychological profiles" about American voters, using a large pool of "mainly unwitting U.S. Facebook users" (Davies). At the time, the true extent of the data in Cambridge Analytica's possession was not yet clear, which was thought to be based on "likes."

In March of 2018, a whistleblower had come out with startling revelations. Christopher Wylie, a former "political operative" who had been with Cambridge Analytica since its inception, revealed how the company came into existence and how it had meddled with

American midterm elections in 2014 and the presidential elections in 2016. It did this with analytics based on a large amount of Facebook data, which the company acquired through a Cambridge University professor. The amount of information about people's behavior that could be inferred from this dataset was "weapons-grade" technology, and was much more powerful than the company admitted at first (Amer and Noujaim).

Later in that same month, the British news program Channel 4 News revealed some inflammatory quotes from Cambridge Analytica CEO Alexander Nix through their own investigation. In an undercover interview with disguised journalists, Nix claimed credit for Donald Trump's victory in the 2016 elections. Through targeted advertising, proxy organizations with automated social media messaging, and specifically focusing on the "Crooked Hillary" brand, they made sure that Trump won the electoral vote (Channel 4 News). Everything they did was powered by their massive data operation, which included the trove of information gathered via Facebook.

Another CA executive boasted about other ways to get their candidate elected. Apart from boosting the candidate they wanted to win, they also focused on other organizations or candidates that participated in an election. In order to do this, they would feed misinformation to the right people, in order to create a different narrative that existed separately from their candidate. This would then "infiltrate the online community and expand with no branding," making it untraceable to its original source (Channel 4 News).

Originally, Cambridge Analytica was founded as a pilot project to "poll voters and test psychographic messaging" in the 2013 gubernatorial race in Virginia (Rosenberg et al.). A group of conservative thinkers, including Breitbart chief Steve Bannon, were interested. Even though the Republican candidate in that race lost, the original backers of the project were still confident

in its success. They needed a source that provided more and better data, and eventually Christopher Wylie found what he needed at the Cambridge University Psychometrics Centre (Rosenberg et al.).

The person responsible for building a working Facebook app was psychology professor Aleksandr Kogan. After the Cambridge University's Psychometrics Centre refused to work with CA, Wylie approached Kogan directly, who worked for that university at the time. He had a license from Facebook that permitted him and his company Global Science Research to gather survey data for academic purposes. That is also what the fine print in Kogan's app read to users. Under the guise of research purposes, Kogan supplied more than 50 million user profiles to Cambridge Analytica, of which 30 million contained enough data to create "psychographic profiles." Interestingly, Kogan maintained his app was not special at all and just a "vanilla Facebook app," implying that anyone could build a similar app and gain the same kind of access to users' data (Rosenberg et al.).

In May of 2018, Cambridge Analytica announced it was shutting down. Both the American company and its British counterpart SCL Group started procedures to apply for bankruptcy. In its statement, the company still held that it did nothing wrong and blamed the "siege of media coverage" for driving away all its business (Contiguglia). Naturally, none of its customers wanted to remain associated with the company after the negative publicity surrounding the revelations about their data collection, leading to an imminent end of their commercial activities.

Even after Facebook shut off access to user data for most companies, a "whitelist" of companies was still given special treatment when advertising on Facebook (The Guardian). This list included multinationals such as Nissan and Royal Bank of Canada and permitted them to

advertise more precisely to users on the Facebook platform. Among others, the list gave them access to phone numbers and other personal data. One of those metrics is the so-called “friend link,” that allowed advertisers to map the degree of “closeness” a user has with specific Facebook friends (The Guardian).

In September of 2018, another security leak in Facebook was discovered, potentially affecting over 50 million accounts, including those of several Facebook executives. The bug involved abusing the “View As” feature that allowed users to display their profile the way another user would see it. The digital access tokens that Facebook temporarily assigns to the user when using this feature could be hijacked by an attacker, giving them full access to the profile that the token belonged to (Isaac and Frenkel). Ironically, the breach occurred in a tool that was meant to let users double-check their own privacy settings.

If things could not get any worse for Facebook, yet another security breach was discovered the following month. Kashmir Hill, an investigative writer for the technology website Gizmodo, discovered that Facebook used users’ so-called “shadow contact information” for advertising purposes (Hill). This information, usually consisting of your phone number, is used to protect accounts against attackers by verifying a person’s identity through secondary means, in addition to a username and password. Facebook could, for instance, send you a text message to determine whether it is really you trying to log onto your account. Another common way of multi-factor authentication is filling out a time-based code from an app, usually installed on a user’s smartphone. A potential attacker will need access to that device and will not be able to obtain access to an account with just the user’s credentials, as they will also need to enter a code generated by the user’s authentication app.

These incidents prove that Facebook still has a long way to go with regards to the security of its users and may need to change its attitude toward user data to ensure long-term security. Mark Zuckerberg was called to testify before Congress in April of 2018, to answer questions regarding the Cambridge Analytica incident (Watson). During that hearing, Zuckerberg admitted that the company could do better. He believes that Facebook did not do enough to prevent tools, such as the one used by CA, from "being used for harm." Zuckerberg also admitted that the company should have banned Cambridge Analytica in 2015, when the company was active on the platform to work for Ted Cruz, among others.

American Studies scholars have dealt with the subject of privacy in various contexts before. A 2018 publication by Sarah Elizabeth Igo, *The Known Citizen: A History of Privacy in Modern America*, documents the evolution of the concept throughout American history. In her book, she talks about the questions raised by contemporary Americans about being "known," in contexts of "profit, security, […] social welfare or scholarly research" (Igo, *The Known Citizen*). The book deals with the various existential parameters of being a "known" American citizen, to what extent Americans should reveal about themselves, and what aspects of a person are "worth knowing," and to whom. *The Known Citizen* charts the course of privacy recognition and scholarship starting in the nineteenth century and will serve as a guide in this thesis in talking about the ways in which privacy has become a staple of American society.

The relationship between citizens and the federal government with regards to privacy has been explored in detail, *The Known Citizen* being a good example of that. However, with an increasing amount of data being gathered by technology companies, their power, presence, and prominence in society has grown. Arguably, Facebook possesses more data on Americans' daily lives, habits, and other personal info than the federal government could ever hope to have. This

creates a situation in which the relationship between an individual and a private entity is akin to that between a citizen and its government. Scholars from various disciplines have articulated this relationship in different ways, which will serve as a lens through which we can view Facebook and the relationship it has to its users.

Something American Studies has not yet addressed, however, is analyzing where harm and privacy intersect. A case study like Cambridge Analytica is a good candidate for such an examination. Not only did the company violate many users' privacy, it also served as a demonstration of just how much personal data is accessible via the platform. This data, even though personal in nature, can be used and abused to influence large groups of people. It also begs the question of whether anyone suffered harm when their privacy was violated.

Not much in the way of scholarship has been written on the parallels between technology companies and governments. However, the power relations both entities have with citizens are becoming increasingly similar, which means the responsibilities of these companies are growing along with that. The most important thing they have in common, is the sheer amount of personal data they hold on their customers or citizens. This makes them morally and legally responsible for what happens to that data.

Marietje Schaake, a former Dutch member of the European parliament, aptly outlined some of these responsibilities and the challenges to legislating them in a 2019 opinion article for *Bloomberg*. She acknowledges that talks on regulations for “behavior in cyberspace” at the United Stations are not progressing as fast as they should. Similar talks at the World Trade Organization regarding rules for electronic commerce are not leading to any fast results either. According to Schaake, this is partially caused by the resistance against “multilateralism,” making it difficult to reach any sort of compromise between different nations on complex issues like this.

Another obstacle is the challenge in creating laws that apply "across jurisdictions," as companies are often based in different countries than where their users live (Schaake). This is why laws such as the General Data Protection Regulation take years to draft and adopt, as the different countries subject to it have to make sure it is compatible with their own national laws.

On the other hand, technology companies seemingly started to take their responsibility to internet users more seriously in April of 2018, when they signed a "Cybersecurity Tech Accord" (Schaake). Thirty-four companies, including Facebook, came together to draw up an agreement consisting of four principles. These, in summary, state that all participating companies should work together to protect users, stop cyberattacks, and work together in order to contain threats in cyberspace (Smith). Whether this initiative was set up with truly altruistic motives or as a savvy business move, it is a sign that private companies are shouldering a part of the responsibility that traditionally lies with a government. That also means that they "must expect to be held to account as governments are," as Schaake points out.

First, we must define what harm means and how we can properly frame the Cambridge Analytica incident in that specific context. For this, we can turn to the harm principle, an important theory within liberalism that originated in the nineteenth century. This principle talks about the relationship between an authority (the government or society in general) and its citizens, specifically when this authority should be allowed to interfere in the lives of those citizens. Along with the potential for harm, the privacy of many people was violated because their personal data was accessible outside of their own control. Because of that, it is important to talk about what privacy means in modern America, how that definition came to be by looking at its history, and where privacy is going in the digital era. In what ways did the Cambridge

Analytica scandal trigger the harm principle and how has it influenced the privacy debate in the United States?

The Harm Principle

Before we can even begin to think about whether anyone suffered harm and what the implications of that harm are, we must first gain an understanding of what the word means and in what ways the notion is talked about. First, we must define harm as a theoretical concept. An interdisciplinary approach is required in order to understand where the term originated, in what ways it is applied, and how it works in the specific context of personal data and privacy. We must place ourselves in the scholarly discussion surrounding harm and gauge how the term can be applied to personal data and privacy in the digital era.

One of the most prominent ways of thinking about harm as a concept comes from the English philosopher John Stuart Mill (1806-1873). In his essay *On Liberty*, he elaborates on what would later become known as Mill's harm principle. That principle states that "the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others" (Mill and Robson 236). It has since become one of the founding principles of modern liberalism and infers that governments should only interfere with people's lives in order to protect them against harm. Governments cannot simply act for a person's "own good," but may only intrude when the threat of harm is real. A central tenet in Mill's philosophy is that "the individual is sovereign" over their own mind and that "which merely concerns himself" (Mill and Robson 236). The only area of one's life in which a government may interfere is where society is affected, or other people in general. However, the threshold for when interference is justified is a point of contention among scholars.

Mill's *On Liberty* was written in a time period characterized by a slow transition from aristocratic societies and sovereign monarchies to more democratic forms of government. Mill realized that giving power to a dominant majority could have the same disastrous consequences

for individual freedom that a single, all-powerful monarch could have. He feared that "informal mechanisms" of groupthink and social pressure could smother freedom of thought and expression (Macleod). From this perspective, *On Liberty* was written, with the central argument being that the only reason a group of people should come together and form a government with a legislative body is to protect the individual from harm. Ideologically speaking, Mill claimed to think along purely "utilitarian" lines. To him, his ways of thinking about liberty were the next step for a "civilized society." Until a society frees itself from the chains of aristocracy, citizens cannot be truly happy, and all that remains for them is "implicit obedience" to a monarch (Macleod). A government should serve the interests of its subjects by intervening only when harm is threatened, and otherwise leave them to their live their lives as they themselves see fit.

However, scholars often disagree on how to interpret Mill's ideas. One of the problems scholars have with Mill's text is that he fails to give a proper definition of what limits and constitutes the word "harm." Because nearly any action can potentially have consequences for others, it is important to limit the scope of what harm means when talking about the harm principle. This issue is a "central problem" in Mills' definition of liberalism and remains a source of contention among scholars. In discussing harm, scholars generally state various conditions that have to be met in order to something to qualify as harm, such as "perceptible damage experienced against one's wishes" (Turner 299–300).

Although the threshold for what is "harm" might be up for debate, academics do agree that harm needs to be quantified one way or the other. If there is no limit to what constitutes harm, the theory cannot be applied to any specific case study, making it useless for any analytic purpose. It is not the case that every negative consequence of one action constitutes harm, and by extension, triggering interference from society or authority (Turner 300). The arguments made

by scholars, however, regarding the circumstances of when interference is warranted, are more complex than simply stating that an action is harmful or not. Some scholars believe that the definition of harm needs to be restricted to specific types of harm. According to Piers Norris Turner, examples of these restrictions are "injury to the vital interests of others," "violation of vital interests of others, and not […] less weighty matters," or "perceptible damage experienced against one's wishes" (Turner 300).

One of the least "restrictive" definitions of harm comes from philosophy scholar Jonathan Riley. The term restrictive, in this case, can be interpreted as not placing any limit on individual freedom, as long as that individual does not harm any others (Riley, *The Routledge Guidebook to Mill's On Liberty* 60). That definition also applies to public goods and spaces, such as the environment. In his understanding of Mill's original essay, he explains harm as "perceptible damage", both to people and to "objects of concern" to them (Riley, *The Routledge Guidebook to Mill's On Liberty* 69). That definition excludes "mere dislike or disgust," i.e. hurt feelings do not count as harm (Riley, *The Routledge Guidebook to Mill's On Liberty* 61). It also excludes any kinds of harm resulting from consensual interactions between people. Riley does acknowledge the ambiguity in Mill's essay but points out that Mill himself discusses feelings with regards to harm. He references a complaint by Mill, in which he says he thinks it is unreasonable for "mere likes and dislikes" to determine to what extent a person should be "free from coercion" (Riley, *The Routledge Guidebook to Mill's On Liberty* 61).

The harm principle, in Riley's understanding, is at its core a "utilitarian form of argument" (*The Routledge Guidebook to Mill's On Liberty* 62). It should not be used as an "abstract right," but instead serve the cause of "general utility," meaning it should work for the common good of people, rather than be based on an ideological notion of what is right and

wrong (Riley, *The Routledge Guidebook to Mill's On Liberty* 62–63). That utilitarian argument for the common good then becomes an equation of weighing the benefits against the negatives of societal interference. One example of this is when a government chooses not to interfere with the economy of a country or specific business, because interfering would do more harm than it would prevent. Even though one company might do harm because it managed to get itself into a monopoly position, the sheer benefits that its success yields for everyone could outweigh that harm. Of course, if this "laissez-faire policy" starts to cause "grievous harm" to individuals (employees or customers, for instance), the harm principle justifies intervention to stop this (Riley, *The Routledge Guidebook to Mill's On Liberty* 63).

Piers Norris Turner argues for another perspective altogether. Instead of trying to find different nuances to define what harm means, he reasons that that nuance is unnecessarily complicating the harm principle (Turner 300). Mill used the word harm to refer to negative consequences in general and did not intend for it to be qualified with various factors. The harm principle, according to Turner, fundamentally has an "antipaternalist" function (301). Instead of looking at the harm principle as a "sphere of personal liberty" surrounding the individual, it serves as a lens through which society (and by extension, the government) should interact with the individual. In Mill's view, authorities should not interfere with individuals based on jurisdiction alone, in order to preserve the value of "free discussion and individuality" (Turner 326). The harm principle should not be read as an explanation of "the whole of Mill's defense of liberty," but interpreted as part of his "broader defense" of that (Turner 301).

According to Turner, the most common interpretations of "harm" do not properly convey what Mill meant when he wrote *On Liberty*. One of the leading views is that of rights violation, in which the harm principle is invoked when a person's actions intrude upon another person's

rights, which is how the phrase "harm to others" is commonly understood (Turner 302). Determining when the harm principle is invoked in that situation is a "balancing of concerns and duties." In Turner's opinion, the end result merely justifies any interference caused by the harm principle, but cannot be used to find the "jurisdictional trigger" for that interference (309). The rights violation approach is useful to defend a harm principle as the existing scholarship has explored; it just cannot be attributed to anything Mill may have said.

The second misinterpretation of harm is that of "perceptible damage," which is where Turner disagrees with Riley. As mentioned before, according to Riley, the harm principle excludes "mere dislike," effectively making it impossible for any authority to regulate "very offensive actions or ways of living," thereby securing "a significant set of actions from social interference" (Turner 310). However, Riley foregoes the "commonsense distinction" that there are examples of being extremely disturbed by another person's actions without suffering any physical harm, but still having one's well-being diminished (Turner 310–11). Continuing the same train of thought, Turner wonders whether other people's opinions, especially the negative ones, can count as harm to an individual. Even though harm of this kind would not induce any interference from an authority, Turner argues that opinions of contempt from others still constitute harm, even though it would not fall under Riley's "restricted conception of harm" (Turner 312). At the same time, the harm principle does not justify society's interference in cases of "mere unfavorable judgment," because that in itself does not constitute harm, even when wielding the broadest of definitions when it comes to harm.

Riley responds to Turner in a 2015 article in *Ethics,* where he argues that Turner makes a "fatal mistake" in his argument regarding the inclusion of "displeasure or distress." In Riley's opinion, expanding the notion of harm to these types of harm turns Mill into "an illiberal

utilitarian," which is incompatible with his writings ("Is Mill an Illiberal Utilitarian?" 783). He believes Turner missed parts of *On Liberty* that would have refuted his own views. Turner talks about how the opinions of other people are not a justification for interference based on the harm principle but foregoes Mill's statements on how an "individual's self-regarding qualities" affect the feelings of others. A person can act in such a way that makes others judge him as being "inferior," but according to Mill, these "self-regarding actions" do not directly cause harm to others ("Is Mill an Illiberal Utilitarian?" 784).

Because of the way Turner conceives of harm, he portrays Mill as "illiberal," in particular because he claims that "feelings of displeasure or distress" count as harm. However, Riley admits that a reading of Mill in which Turner's arguments are correct is possible. Before going on to give evidence to the contrary, however, he emphasizes that there is more "textual evidence" that proves Mill is, in fact, the liberal he is portrayed to be (Riley, "Is Mill an Illiberal Utilitarian?" 786). "Mere displeasure" can never be a reason for "coercive interference," according to a quote by Mill: "But to be restrained by others in things not affecting their good, by their mere displeasure, developes [sic] nothing valuable except such force of character as may unfold itself in resisting the restraint" (Riley, "Is Mill an Illiberal Utilitarian?" 786). In other words, society would consider interfering with individuals displeasing others if it were harm but interfering with such a person will lead to more conflict than that which society is trying to solve.

Riley argues that Turner's viewpoint of the harm principle being "antipaternalist" does not correspond with Mill's writings. For Turner, that antipaternalist function is what makes Mill a liberal, but Riley disagrees. Although a mature, sound of mind person's own good is not enough by itself to justify society's interference, it can be a contributing factor in determining "a sufficient warrant" for that to happen. What a person does to or for himself can never be a

sufficient reason on its own, because it does not cause any "nonconsensual harm" to anyone else (Riley, "Is Mill an Illiberal Utilitarian?" 794–95).

Bernard Harcourt, a legal scholar, maintains a perspective similar to scholars from other disciplines on the differences between types of harm, but approaches it from a different discipline. He argues that the harm principle, as set out by Mill, served "only as a threshold determination," a line that is nowadays crossed in most judicial situations in which harm was allegedly done to a party, especially when compared to politics of the 1960s. Because of that, the question of whether harm was done does not exist anymore or has become irrelevant at the very least. The harm principle does not offer any distinction between types of harm or the total amount of harm done. In Harcourt's opinion, this development has led to the "collapse of the harm principle," as it no longer acts as a "limiting principle" (Harcourt 114–15).

Harcourt illustrates his point by giving an example from 1998, where several neighborhoods in Chicago voluntarily voted themselves dry (109). All bars and stores that sold liquor closed up shop, essentially banning the sale of alcohol in the area. In this procedure, a post-Prohibition law was invoked, making it possible for districts to give up alcohol of their own accord, without it being forced by law.

Richard Daley, the mayor of Chicago at the time, led a campaign to gentrify the neighborhoods that would eventually vote to close liquor businesses. However, his rhetoric did not focus on the "morality of drinking," but on the harms caused by the substance. He is quoted to have said that it was a quality of life issue, rather than an attempt to impose prohibition, exemplifying the focus on the negative physical consequences of drinking instead of the abstract moral implications (Harcourt 110).

The threshold for what constitutes harm has shifted along with the focus from moral to physical implications. Harcourt illustrates this with an example from law enforcement, as the debate regarding how to deal with loitering has shifted significantly in the second half of the twentieth century (155). Where loitering used to be regarded as merely undesirable in most contexts, courts on multiple levels began distinguishing between different types of loitering in that period. In many places, the laws were changed to only criminalize harmful loitering, as opposed to punishing citizens for any type of loitering (Harcourt 157). After all, simply being in a specific place for no reason does not cause any direct harm and should by extension not be considered a crime.

This way of thinking shifted after the influential 1982 essay "Broken Windows" was published in *The Atlantic*. In this essay, the argument was made that even innocent, non-criminal loitering can lead to undesirable behavior further down the line. "Untended property," referring to abandoned cars or buildings that have no owner, can attract unwanted attention, leading to an overall increase in crime in that area. These circumstances can lead to a cycle of increasing crime that reinforces itself in different ways. Not only do the physical circumstances invite criminal behavior, but residents will also act differently. For instance, they will go out on the street less and actively avoid other people (Kelling and Wilson). Through that, the "neighborhood" stops existing and turns into a place where people merely live, rather than form a community. This is not a guarantee that crime will occur, but it does become more likely because there are fewer "informal controls," meaning that people are less concerned with each other's actions (Kelling and Wilson).

Mill admits that there must be limitations to the harm principle, as no one person lives apart from society. Even if individuals ideally live free and autonomously without external

interference, some personal choices can cause harm, both to others and the self. For instance, a person should be free to drink alcohol as often and as much as they want, even though overindulging can lead to health problems. However, this behavior should only be punished if that alcohol consumption leads to harming others (Mill and Robson 43). People with certain jobs, such as military personnel, should not be permitted to consume alcohol when at work. Since it is their job to protect citizens, alcohol consumption will only lead to harm those "fellow citizens" (Mill and Robson 43).

However, the harm principle also serves to protect those who are incapable of "self-government," such as people who have not yet come of age and those who are not sound of mind. "Indulging" in activities as "drunkenness" can be interpreted as a sign of being unable to govern the self and could be considered as an obstacle to happiness. For Mill, in such a situation, the government should ask itself whether it is possible to prevent these persons from doing harm to themselves (Mill and Robson 43–44).

According to Harcourt, Mill held an inconsistent stance on alcohol consumption and the way in which its sale should be regulated. He was against restricting the total number of places where alcohol could be sold, but advocated for regulations on the ways in which they should be operated (Harcourt 168). The main problem here is that Mill associates alcohol consumption with crime, at least to an extent. In this case, he is not consistent with the other examples he refers to regarding the harm principle.

The harm principle as described by Mill traditionally deals with the relationship between a government and its citizens. The same association occurs when thinking about how technology companies relate to their users. After all, they are the keepers of a wealth of personal data, which gives them a specific kind of power. Governments in Mills' own lifetime could only dream of

the information a technology company like Facebook has on its users. Not only does Facebook know who a person associates with, they also know a person's interests, both personal and political. A nineteenth-century government with that kind of knowledge would have been considered tyrannical to say the least.

Thinking about personal data in the context of harm raises several questions. Personal data can be talked about in several ways. One of these is considering it as a good, as a property that is palpable and can belong to someone. This also means that it can be traded between interested parties. Paul Schwartz warns, however, that the "propertization of personal information" can only be done to a certain extent (Schwartz 2088). As soon as this practice undermines a common understanding of privacy, however, "personal data trade" becomes impossible, as it is not sustainable, leading to a "privacy market failure" (Schwartz 2088).

Another argument against trading in personal data is a seemingly "paternalistic" one. This critique on the harm principle has been said before, and in this context, relates to the way people treat their own data. Even in 2003, scholars were considering that individuals "may prove incapable of […] managing property rights in information." Mismanaging data as a good certainly exceeds the threshold of the harm principle, regardless of what specific criteria one applies to it (Schwartz 2088–89). Apparently, even before the age of social media and large databases of personal information, concerns regarding the ways in which people manage this information were ever present.

Schwartz makes a distinction between privacy as a social good and as an individual good. This means that privacy can be considered in the context of an entire society (for instance, through law), but also with regards to "individual self-determination" (Schwartz 2087). Privacy is necessary for citizens to participate in democracy, because without it, there can be no private

"deliberation" about political ideology. Without it, there can be no consensus, and by extension, no republic (Schwartz 2087).

In the following section, we will consider the role of privacy in the United States since its inception. Before we can make any determination as to what the role of privacy is in the Cambridge Analytica scandal, an overview of privacy must be sketched out. This is necessary to gain an understanding of where the debate originally started, what the relationship between society and privacy is, and to determine if we can say something meaningful about where the debate is going in the future.

Privacy in America

Privacy has been a fundamental part of the lives of Americans ever since the first colonies were founded in the New World. In a way, privacy could be considered one of the main reasons why the first settlers set sail across the Atlantic in the first place. The Puritans, for instance, were one of the first groups of Europeans to colonize what is now known as New England. They originally set sail for the New World in order to escape religious persecution in Europe. In other words, they moved away from a system that did not respect their religious privacy.

It must be noted that the relationship between the Puritans and other churches in their homeland of England was more complicated than a mere disagreement regarding ways of worship. For some Puritans, at least, the Reformation of the Church of England did not reform fast enough or did this in ways that were unacceptable to the Puritans. For example, Puritans had different ideas about marriage, and believed the Church of England put too much emphasis on the spirituality of the concept, without being able to provide any biblical justification for it (Hochstetler 490–91). Eventually, groups of Puritans decided to emigrate to the American continent. The first colony to be established was the Plymouth Colony, founded by a group called the Pilgrims (Bremer 15–16).

After the American Civil War, two concepts began to take shape in the minds of Americans. One of these was the "status of the private person," which meant that individuals began to think of themselves as individuals with private thoughts and properties, that were under pressure from authorities. The second concept came along with that status, as Americans began to call for "a right to privacy" (Igo, *The Known Citizen*). As a result, almost every important

technological or sociological advance since that time was considered with regards to the implications for Americans' privacy.

As laws are often created through disputes in the United States Supreme Court, it is imperative to analyze the most important ones in order to gain an understanding of where the privacy debate is at in modern times. In this chapter, we will explore a number of Supreme Court cases that served as important milestones in the privacy debate, in order to establish what kind of impact the Cambridge Analytica incident may have for Americans and what could happen in the future when it comes to digital civil rights and the protection of information in the digital realm.

It is important to note that exploring the differences in privacy attitudes between different regions of the world warrants a separate study and is beyond the scope of this thesis. Those differences are not only cultural but can be found in other aspects of society as well. Glancing over them in a paper dealing with a specifically American incident within American Studies would not do the subject justice. As law scholar Whitman remarks, "we do not seem to possess general 'human' intuitions about the 'horror' of privacy violations […] We possess American intuitions – or, as the case may be, Dutch […] or German intuitions" (1160).

In the period after the American Revolution, both in Europe and the newly formed United States, people started thinking about the relationship between their government and their personal lives. This not only resulted in philosophers like John Stuart Mill coming up with theories about harm, but also affected domestic relationships within American families. Ruth Bloch wrote an essay detailing the period between the American Revolution and the mid-nineteenth century and how attitudes toward domestic abuse changed.

Wife beating, a frequently occurring example of domestic abuse, was a tradition that predominantly originated in England, records of which go back as far as the seventeenth century

(Bloch 231). In the American colonies (and later, the United States), a trajectory of legislation can be traced starting in that period that led to opportunities for women to defend themselves against any abuse from their husband. Especially in New England colonies, Puritan communities would resort to "legal sanctions" to ensure that men in families behaved religiously responsible. Although it may look like these women were protected to an extent by the law, Puritan legislation went both ways: wives were also disciplined if they did not act the way they should (Bloch 232).

The origin of this judicial system lies with the English monarchial system. Violence between "subjects" did not affect any members of the royal family or "infringed on their authority," so therefore was not a criminal matter. Only "injuries to the king's realm" were considered as a public matter, and by extension, as a criminal case. Battery and assault cases between free men were handled as a civil case between individuals, meaning that prosecution came out of one's own pocket. However, when the peace was significantly disturbed due to a violent incident, a magistrate would force those involved to compensate the victim, the court, and pay for any damages caused (Bloch 236–37). This phenomenon served as a precursor to philosophical thinking about the role a governing entity should play in the lives of citizens. John Stuart Mill and his harm principle could be considered a result of the societal shift from the family to the individual, and from a monarchy to a republican style of government.

The civil way of handling disputes by paying a fine did not apply to women, however. Their only recourse when dealing with their violent tendencies was through the criminal system and litigating for "breach of the peace," because abusing one's wife was considered an injury to "the king's realm" (Bloch 237). Especially when a husband would inflict permanent injury on his wife, it would be considered a breach of public peace instead of something that occurred in the

private sphere. This way of thinking painted the kingdom or commonwealth as the victim, instead of the individual. The other option wives had was filing for divorce, but violence on its own was usually not considered a good enough reason to go through with it.

After the Revolutionary War, the family as an institution was still an important part of American society, but shifted from a public to a more private domain "distinct from government" (Bloch 238). This meant that abuse was no longer regarded as a violation of public peace, making it more difficult for women to sue their husband for the crime of abuse. To make matters worse, some husbands sued their wives for desertion if they left them, regardless if they were abused or not (Bloch 237–38).

On the other hand, many states introduced new divorce laws in the years after the War, making it easier to get a divorce in cases of abuse. Thanks to these laws, dissolving a marriage became a matter between two individuals rather than a state affair. It also marked a departure from the legal system that originally came over from England, where the power to grant divorces was granted exclusively to the English parliament (Bloch 238). In broader terms, the British monarchy controlled almost every part of the government and was able to influence it, including parliament, in many ways.

One of the main challenges in talking about privacy as an abstract concept is that the term is used in a wide range of academic fields, and by extension, can mean different things depending on the context in which it is used. Debbie Kasper acknowledges that even though a "desire for privacy" is a universal human trait, it is difficult to arrive at a "fundamental definition" because the context is always different when talking about the concept (70). However, such a definition is necessary in order to use privacy as a theoretical concept. Whether a universal definition can be formulated, however, is up for debate.

Igo argues that the idea of a "stable definition" of privacy should be abandoned altogether. In her opinion, the term's meaning varies per time period, and should be judged according to the ways in which Americans thought about it at the time. It has been used as a "catch-all" to deal with new technologies that changed the way society was organized, such as new forms of media and shifts in what was public and what was private. The term privacy is defined by a "bundle of ideas," that cannot be considered as "transhistorical or ahistorical," but should instead be carefully weighed against its context (Igo, *The Known Citizen*).

Even though privacy as an idea played a role in the early beginnings of the United States, it was not until the late nineteenth century that it was first discussed in an article by Samuel D. Warren and Louis D. Brandeis in the *Harvard Law Review*. This article first introduced the "right to be let alone," as a logical consequence to the "right to enjoy life" (Warren and Brandeis 193). This right came along with an extension of what the word "property" meant, to encompass both material and immaterial possessions. According to Warren and Brandeis, this was a natural consequence of human progress. After mankind realized that "only a part of the […] pleasure and profit of life" comes from that which is physical, it was only a logical consequence that the other part, consisting of "thoughts, emotions, and sensations" would also be protected under the law, alongside physical possessions (Warren and Brandeis 195).

"The Right to Privacy" was a revolutionary text for its time, and it is still part of the privacy debate in modern times (Igo, *The Known Citizen*). It was referenced in the well-known court 1928 Supreme Court case *Olmstead v. United States*, in which Brandeis served as an associate justice. In that case, the Court ruled that the fourth and fifth amendments were not violated when Roy Olmstead's private phone was wiretapped and used as evidence against him. Justice Brandeis wrote a dissenting opinion in that case, in which he criticized the court for

refusing to establish a constitutional "right to privacy," citing his own publication from 1890 and stating that this right is the "most comprehensive of rights and the right most valued by civilized men" (Igo, *The Known Citizen*).

According to law scholar Anuj Desai, the history of "communications privacy" can be traced back to even before Warren and Brandeis' 1890 text. One of Brandeis' cited precedents in the *Olmstead* case in particular, *Ex parte Jackson* (1877), had far-reaching consequences for privacy in the postal system (Desai 556). In this case, the Court upheld the Fourth Amendment in that the government was not allowed to open sealed letters without first obtaining a warrant.

Desai lays out several arguments as to why it is still a relevant case today. First, it is one of the earliest examples of the Supreme Court holding the federal government to the Constitution when it comes to communications privacy. The second argument is that *Ex parte Jackson* shows how constitutional law can reaffirm "legislative choices" (Desai 557). In this case, a Congressional policy that set up the American postal system with specific attributes in the eighteenth century, effectively became constitutional law a century later by means of this court case. From its early beginnings, the American postal system was setup with "privacy of correspondence" in mind. In *Ex parte Jackson*, the Supreme Court wrote this feature into law by forbidding the government from opening sealed mail without first obtaining a warrant (Desai 557).

As with other examples, the American post office has its origins in a British precursor. This postal system was controlled by the British government, and served as an "intelligence organ," based on a "royal prerogative" that permitted the post office to spy for the crown (Desai 560). This gathering of intelligence occurred through the so-called "Secret Office," that manipulated the flow of mail and intercepted correspondence where necessary for the British

state. Even though a warrant was required for each individual instance in order to do this, officials justified intercepting mail through a 1765 general warrant that ordered all "diplomatic correspondence" to be sent to London (Desai 560). It was even customary for British state officials to send lists of names to the post office in order to gain insight into what they were writing in their correspondence. The people targeted by these actions would often be political opponents or "patriot" citizens that were considered to be a nuisance to the British realm (Flavell 403).

This policy was instituted after the British government grossly misjudged the amount of support they had in the American colonies when the Revolutionary War began. After the Seven Years' War took place in Europe, the continent stopped working together in so-called "transatlantic interest groups," which were an important source of information for the British government regarding the colonies in the New World (Flavell 404). This led to a gross "failure of understanding" regarding the perception people in the colonies had of their British overlords. Whether they blamed King George or his government is up for debate, but that the British were driven out as "villains" by the "good" Americans is the leading narrative in historical scholarship regarding the war. Upon closer study, however, King George did not take much interest in affairs surrounding the American colonies, and many of the events leading up to the Revolutionary War were a result of "confusions and factional rivalries" in his administration (R. R. Johnson 339–40).

It was not until 1965 that the first signs of privacy rights for individual citizens were constitutionally decided at the United States Supreme Court. What is interesting about these landmark cases is that many of them were about sex. Rubenfeld explains that even though it was nowhere explicitly mentioned that sexuality was important to privacy doctrine, that is what it

gravitated around (Rubenfeld 744). In *Griswold v. Connecticut* (1965), the Supreme Court ruled that a state law preventing married couples from using contraceptives was unconstitutional. According to the majority opinion, the "right to privacy" can implicitly found in the "penumbras" of the first, third, fourth, fifth, and ninth amendments to the Constitution. This meant that two married people should be permitted to make them own choices regarding what they do in the "privacy" of their own bedroom (Rubenfeld 744–45).

Even though there are more cases related to privacy in this time period, most historians agree that *Griswold v. Connecticut* was one of the landmark cases that cemented privacy in constitutional law. According to Igo, this was the case "that would finally supply privacy its constitutional bona fides." Other cases that came before *Griswold* were edge cases that did not apply as broadly to "personhood," and did not do as much for the right to privacy as *Griswold* did. It was especially expected that *Griswold* would provide significant privacy protection against "electronic eavesdropping." The *Duke Law Journal* wrote an analysis of *Griswold* in 1966 and pointed out the possible consequences for electronic surveillance. In that same analysis, the author acknowledged that the "now partially secured constitutional 'right of privacy' remains open to conjecture," referring to the discord among the justices in the case ("Constitutional Law").

Igo points out that the case was not as clear-cut as it might appear. Seven out of nine judges agreed that the Connecticut state law should be struck down, but they did not reach agreement as to why it should be scrapped. Some felt the law was incompatible with the first amendment, others believed a "right to privacy" was inherently present in the Bill of Rights all along (Igo, *The Known Citizen*). The two remaining judges believed the law was "an uncommonly silly law" and "obviously unenforceable, except in the oblique context of the

present case" (Sutherland 286). This disagreement among justices is one of the reasons this case is of great interest to scholars. According to law scholar Arthur Sutherland, it is an "extraordinary thing" for a court case to witness such "divergencies in the theories of the Justices who wrote the opinions to explain it" (285).

In 1967, another landmark case was decided in favor of privacy rights. In *Loving v. Virginia*, the Court overturned a Virginia state law that dictated that interracial marriages were illegal. States were not permitted to interfere with "an individual's choice of whom to marry," as it violated the Equal Protection clause of the Fourteenth Amendment. That clause states "nor shall any State […] deny to any person within its jurisdiction the equal protection of the laws," which was ruled to apply to people of all races (Rubenfeld 745). This clause dictated that both state and federal laws applied equally to every American, regardless of economic conditions, gender, or political affiliation. After this case, it also became easier for the less affluent to marry, as there were several state laws that prevented poor people from marrying or suing for divorce.

After the *Loving* case, privacy legislation was seemingly limited to married individuals only, but that came to an end in the 1972 case *Eisenstadt v. Baird*. In this case, the Court rephrased privacy rights from previous cases as "the right of the individual […] from unwarranted governmental intrusion into matters so fundamental" (Rubenfeld 746). According to the Court, a Massachusetts law that made it illegal to sell contraceptives to single people violated the Fourteenth Amendment and was declared invalid.

In the same year as *Loving*, the right to individual privacy was finally acknowledged by the Supreme Court in *Katz v. United States*. That case dealt with the question of whether a public phone booth was considered private under the Fourth Amendment, as a man named Charlie Katz was wiretapped by the FBI through such a booth (Igo, *The Known Citizen*). Katz used this booth

to place illegal gambling bets but was acquitted by the Court because of the way the FBI obtained the evidence used in the case. The privacy protection that the Fourth Amendment granted to properties, was now extended to people as well. According to Alan Sklansky, it became "conventional wisdom" that the Fourth Amendment was about privacy, even though the majority opinion in *Katz* claimed that this amendment "cannot be translated into a general […] 'right to privacy'" (1075). This train of thought emerged from the case's concurring opinion, written by Justice Harlan, who wrote that the Fourth Amendment provided expectations of privacy "that society is prepared to recognize as reasonable" (Sklansky 1075).

Another landmark case for privacy in the United States is the well-known *Roe v. Wade* case that was decided in 1973. In this case, the Court ruled that a woman is protected by the Constitution in their choice to have an abortion or not. One of the arguments made by Justice Blackmun was similar to that of earlier cases. The Fourteenth Amendment was ruled to be "broad enough to encompass a woman's decision whether or not to terminate her pregnancy" (Ziegler 297). Mary Ziegler notes that *Roe* was also a landmark case by focusing on rights-based arguments, rather than policy-based. It specifically dealt a blow to arguments based on population control, which shifted the narrative surrounding abortion. Before *Roe v. Wade*, the "population control movement" supported abortion, but mostly as a "colonial economic interest." By using constitutional rights as an argument, rather than so-called humanitarian concerns, the racist undertones of the population control movement were laid bare (Ziegler 299).

As with many of the other court cases mentioned in this chapter, talking about *Roe v. Wade* and its many implications warrants a separate study of its own. Much research has been done regarding the pro-life and pro-choice implications of *Roe*, along with the impact the case has had on women's and minority rights movements. However, since *Roe v. Wade* was an

important case in shaping the privacy narrative in the United States, its contributions to that subject specifically should not be glossed over simply because the case itself is a nexus of various controversial subjects.

Modern day attitudes toward privacy are quite different between Americans and Europeans, which is evident when looking at the ways in which the American judicial system developed from its British origins. Europeans seem to believe Americans do not understand the importance of keeping certain things private at all. For instance, it is not unusual for Americans to ask dinner guests about their salaries or net worth, something that is unheard of in a European context. In a more commercial context, the American way of doing things is also significantly different. A good example is the way in which an American business can access customers' credit history, to determine their trustworthiness in doing business with them. Being able to view a particular person's history would be considered a severe violation of privacy in the eyes of a European, as financial data is protected by law in many European countries (Whitman 1155–56). Americans, in contrast, consider this a way to protect their business interests, as the verification that their business is in good hands outweighs that possible privacy violation.

On the other hand, Americans regard some European practices as strange as well, particularly when it comes to nudity. Both in German and Dutch public life, it is accepted as "normal" to engage in public nudity. Americans, on the other hand, generally do not expose their "privates" in public, and consider this a "baffling" practice, to say the least. Genital nudity especially is considered controversial in the United States, and even in advertising, where many things are tolerated, bare breasts are covered up one way or another (Whitman 1158).

Whitman cites another profound rift between American and European judicial interpretations of privacy. Many Europeans countries have laws that govern what names parents

are allowed to give to their children, which is also in stark contrast to what an American would consider to be freedom from unjust governmental interference (Whitman 1158). In the Netherlands, the law prescribes that public servants can deny parents a certain first name, when that name is in violation of the law or unfit in the eyes of the employee registering the name. For example, a Dutchman cannot give their child a name that is in itself an offensive word, or a name that consists of many other names (Ministerie van Algemene Zaken).

In the technology industry, attitudes toward privacy are often cavalier. The CEO of Sun Microsystems, a company that was later acquired by Oracle Corporation, said in 1999: "You have zero privacy anyway, get over it!" (Kasper 69). This quote, preceding social media by quite a few years, referred to a potential privacy breach in a Sun networking product. He could not have predicted that his quote would later also be used in a social media context, and that people would willingly place much of their personal information on the internet.

Mark Zuckerberg's stance toward privacy has shifted numerous times over the years. He was quoted as saying that "privacy is no longer a social norm" in 2010, because people did not believe in it anymore (B. Johnson). In his opinion, privacy as a social norm evolved due to how comfortable people had gotten with sharing numerous types of information with each other on the internet, thanks to the rise of blogging. That is a significant departure from Facebook's humble beginnings at Harvard, where it began as a tool for private communication among students (B. Johnson).

Zuckerberg's attitude has changed significantly in the past nine years, as the CEO's opinion on what its users think regarding privacy has been practically reversed. During its yearly developer conference, the Facebook director announced that protecting the privacy of its users would become the company's main focus for the near future. He likens platforms such as

Facebook or Instagram to "the digital equivalent of a town square," but says that users want to spend more time in "the digital equivalent of the living room" (Wong, "Facebook Is Pivoting to Privacy"). Zuckerberg does acknowledge that the company's reputation for privacy was "shredded" by dozens of privacy scandals over the years, but he is confident that the company can "evolve." He has high hopes for its new messaging product, in which Facebook Messenger, WhatsApp, and Instagram will be combined. This product is being built "with privacy in mind," a far cry from his attitude a decade earlier (Wong, "Facebook Is Pivoting to Privacy").

However, even in 2010, years before Cambridge Analytica, Facebook's history was littered with incidents that violated the privacy of its users one way or another. One of these was a change in Facebook's privacy settings that made all new posts to the network visible to the public by default. This change was supposed to inspire Facebook users to share more with their friends and was part of an update that gave users more fine-grained control over what they shared with others. In practice, many users posted information about their current city, friends, and likes to the public internet without noticing. Other incidents involved posts made by users that were seemingly placed in a private group but turned out to be visible to the open internet. This incident led to the firing of thirteen Virgin Atlantic employees, who wrote embarrassing messages about passengers and the company's maintenance schedule for its planes (B. Johnson).

As evidenced by earlier incidents, privacy violations regarding data acquired from Facebook can also occur due to user ignorance in another way. Users are not just giving up their privacy by uploading their details to the internet, but researchers or other parties interested in using this data can abuse it, both intentionally and unintentionally, and with or without permission from subjects. What happened after the aforementioned 2010 update and the

Cambridge Analytica incident are only a few examples, but there are other situations that illustrate the dangers of unknowingly uploading one's data to a service like Facebook.

Before performing a social study on Facebook users, some ethical concerns need to be addressed. It may seem straightforward to find data on the internet suitable for research, but there are issues regarding privacy and anonymity that must be tackled before any kind of research can take place. Simply drafting a user agreement with language that supposedly shields user data is not enough, regardless of whether it is done in a research context or when it applies to a social media platform. There is also a significant risk that users will not pay attention to such an agreement, which we will see later on in this chapter.

In 2008, publicly accessible data of the Facebook profiles of a group of college students was used to create a dataset for sociological research. This dataset was designed to be useful for varying types of research, particularly for exploring the relationship between "virtual" and "real life" social spaces (Lewis et al. 330). The dataset that was used in the so-called "Tastes, Ties, and Time" study consisted of everything that was posted to the Facebook profiles of about 1,700 students at an American university. Even though the authors tried to anonymize the data, the group could still be identified, violating the privacy of the affected students (Zimmer 313). This experiment is a good example of the dangers of using data belonging to a group of real people for academic purposes

For the T3 study, researchers gathered information from the aforementioned group of college students over a four-year period, consisting of several datasets sampled per academic year. The public data of about 1,700 profiles was scraped and collected, and connected to "housing data" obtained from the (supposedly anonymous) university at which these students

were located (Zimmer 314). Both Facebook and the university gave permission for the researchers to access Facebook to download profile data.

The T3 study was problematic in several regards right from the start. First, the researchers used research assistants to carry out the data collection from Facebook. These assistants were both undergraduate and graduate students, with varying amounts of access to the profiles. For instance, one RA might have mutual friends with a specific profile, meaning that they get access to more data than someone who is not friends with that profile (Zimmer 318). This leads to a dataset that is inherently skewed, since not all the gathered data is meant to be accessible to the public. The researchers themselves claimed they did not access "any information not otherwise available on Facebook," which is an untrue statement when accounting for the extra information some of the RA's were able to extract.

The second glaring problem with T3 was its lack of anonymity, despite the researchers' best efforts. T3 authors stated that "all identifying information was deleted," but miscalculated how easy it is to use small amounts of data to piece together details about a certain group (Zimmer 318). The dataset contained several students with "unique" properties, such as nationalities, ethnicities or other similar characteristics that made them stand out from the group. Using these properties, their identity could theoretically be easily compromised. With this method, Michael Zimmer identified the dataset as a group of Harvard College students "within days" of its release date (316). The researchers helped narrowing the search down by saying their dataset came from a private college in New England, with a freshman population of around 1,700 students. Those parameters led to a group of seven possible colleges, making it easy to determine which of those was the right one. Several other revealing pieces of information, such

as the choice of majors and the countries of origin of several exchange students were also not omitted from the dataset (Zimmer 316–19).

The T3 researchers drafted a statement containing the terms of use for their dataset, which any interested parties must agree to in order to gain access. The language of that document, however, was problematic in itself. It recognized that the contents of the set could violate subjects' privacy, and therefore demanded that users of the dataset make no attempt to identify students. However, such language is a poor substitute for proper privacy protection and does not come close to protecting personal information as actual anonymization would have.

To make matters worse, a 2002 study by Adam Gatt indicates that most users often accept online terms and conditions without reading the contents. About 64 percent of users accepts terms and conditions immediately, while about 35 percent occasionally clicks away. Only about ten percent of online users read these so-called "click-wrap agreements," without realizing they are entering into a legal agreement with a business by clicking the button that says "I accept" (Gatt 408). It is plausible to assume that in 2019, these numbers will have only gone up, as the internet has become more commonplace, meaning that the number of users with limited knowledge of the internet has increased significantly. On the other hand, it could also be argued that general awareness among internet users regarding the user agreements of internet services has improved, because of how ubiquitous the internet has become.

A 2012 survey among American businesses conducted by a business law scholar portrays a similar trend as Adam Gatt's article, albeit in a different context. About 18 percent of the employees surveyed by Patricia Abril are subject to rules surrounding social media usage in the workplace. However, the study participants in this group feel that these policies are "ineffectual," and little people pay attention to them in their daily work activities (Abril et al. 113). Instead,

employees act in accordance with their company's workplace culture. Informal and "society-wide" norms influence behavior more so than legal documents or prescriptive guidelines do, because the rules often do not correspond with the ways in which people interact with social media (Abril et al. 114). Furthermore, several court cases in the United States have established that the "totality of circumstances" dictate the extent to which an employee should expect privacy in the office. That means that both culture and policy should be taken into account, not just the rules an employee agrees to when getting hired for a job (Abril et al. 115).

Protecting privacy by making users agree to terms and conditions cannot be regarded as proper guarantee against abuse. That goes for the sociologists who conducted the T3 study, but also serves as an important lesson to Facebook. The company has, on occasion, used its terms and conditions to defend some of its behavior by saying users agreed to the terms when they signed up for the service. The latest change to those terms was done at the request of the European Commission, who requested that Facebook clearly laid out in simple terms what the company does with the data from its users and how user profiling works for advertising purposes. The Cambridge Analytica "scandal" was a direct cause of the Commission's request, as it was unclear how the company monetized the data its users upload to Facebook (European Commission).

Cambridge Analytica in Context

As we have seen earlier on in this thesis, the harm principle and privacy are both topics that have extensive bodies of scholarship. Harm is an abstract term, usable as an analytical tool, but also with a historical purpose. After all, it was written to mediate societal changes in government and determine how people were to interact with a democratic society. Privacy, on the other hand, is a concept that is fundamentally present in many layers of American society, both in tangible and immaterial ways. As we established before, its meaning has changed through time, and has been dealt with in the courts in different ways, depending on the issue related to privacy in court.

With so many changes happening in the ways in which people share information, privacy is more important than ever in the twenty-first century. Even with Mark Zuckerberg declared that privacy was no longer "a social norm" almost a decade ago, Cambridge Analytica was a wake-up call in that the data that is out there can be abused. It is ironic though that the people "with a vested interest" in Americans' information sharing are the ones to decry peoples' desire for privacy (B. Johnson).

In *Katz v. United States*, the right to privacy became part of constitutional law, but the terms in which this happened were still vague. Igo points out that the court spoke of a standard of "reasonable expectation," but questions whether that expectation from 1967 needs adjusting for the twenty-first century. Now that information about individual people can be found with a simple search engine query and just about anyone can purchase and operate drones, should that "reasonable expectation" of privacy be adjusted (Igo, *The Known Citizen*)?

These aerial drones are a good example of a comparatively new phenomenon that does not yet have sufficient rules in place on how to deal with privacy. Even though existing laws do

cover their usage to an extent, such as rules regarding photography, but there have not yet been major court cases that regulate drone usage specifically. In the meantime, a "voluntary code of conduct" has been drafted by drone pilots that contains procedures on how to safely operate a drone while respecting other people's privacy at the same time (Kakaes). But because airspace is neither a private nor a public domain, it will need proper legislation in order to prevent "massive violations of privacy by large corporations" (Kakaes). The court cases mentioned in this thesis already defined many aspects of "common law" when it comes to privacy, but they need to be defined in its proper context.

What makes the current judicial situation surrounding privacy so precarious is that there is no specific constitutional legislation that defines how large sets of accumulated data should be treated. Igo calls it "a deluge of volunteered […] personal information, on the one hand, and the increasingly sophisticated capacities of other parties for […] acting on it, on the other" (*The Known Citizen*). The 1970s fear of "not knowing who knows you" has come back in the form of machine learning algorithms that combine a wealth of data to profile and categorize individual citizens. Some scholars have called for a "right to quantitative privacy," along with individual rights to view your own data and "inspect data companies" (Igo, *The Known Citizen*). The European GDPR is a good start on this front, but that is a strictly European law. It is for now unclear whether any comparable American law is on the horizon, and whether current constitutional protects are adequate is up for debate.

One of the things to think about when thinking about the Cambridge Analytica incident in relation to harm, is to consider whether the threshold for triggering the harm principle has been crossed. That threshold has been defined in numerous ways by the scholars cited in this text, and by comparing ideas from different disciplines, the difficult nature of the harm principle has been

established. In the next section, we will look at whether we can say anything useful regarding the threshold for each of the scholars that were discussed earlier.

If we go by Schwartz' relatively simple wording of the harm principle, we can conclude immediately that the harm principle was triggered in the Cambridge Analytica incident. In his view, whenever individuals mismanage information, the harm principle is "exceeded" (Schwartz 2088). In his understanding, professor Kogan simply did not manage the information in his app correctly by selling it to Cambridge Analytica. Arguably, Facebook itself is also to blame here, as it created the circumstances in which Kogan's app was functionally possible.

If we read Riley's understanding of the harm principle, did Cambridge Analytica cross the threshold for harm? Arguably, no. Facebook users did not suffer any "perceptible damage" when their data was being scraped for use in a dataset, even though it was against their will. His interpretation of the harm principle is a utilitarian one that does not take individuals' feelings into account. It could even be argued, in theory, that Cambridge Analytica's successes outweighed the harm they did by using Kogan's data, even though the affected users did not know their data was in that dataset. Only when "grievous harm" is done, should the harm principle be triggered, which is not what happened in this case. Regardless of what happens in people's lives, one cannot say they physically suffered because of the Cambridge Analytica leak.

On paper, Piers Norris Turner disagreed with Riley, and it is feasible that he would disagree regarding CA as well. He argues that a "rights violation" can be considered as harm, which means that the violation of digital privacy is a form of harm. In Turner's opinion, the harm principle is also triggered in cases where people are not physically harmed, but still suffer from a decrease in well-being. Having one's personal data fall into the hands of a data company without

one's consent is absolutely one of those cases, and goes beyond "mere unfavorable judgment" (Turner 312).

For Bernard Harcourt, the threshold for harm would be crossed as soon as harm was alleged, as the principle itself makes no distinction between different types of harm, in his opinion. It no longer acts as a "limiting principle," meaning that the question of whether harm was done or not can no longer be measured through the test of the harm principle.

Yet when we follow his reasoning regarding the "Broken Windows" essay, a comparison can be made with the CA incident. That essay argued that seemingly innocent behavior can "invite" criminal behavior because "untended property" creates opportunity, making it easier for potential criminals to take the leap and do something illegal. A similar situation takes place in the digital realm, as sitting on a big chunk of valuable data along with its potential for monetization can be extremely inviting to persons interested in that data. If it were made physically impossible to do something with that data, potential abuse could be deterred. On the other hand, having access to that kind of data is similar to coming across "untended property."

When the harm principle is triggered, or the threshold is crossed, it is assumed in liberal theory that the government or society will intervene to protect a subject from harm. However, traditionally speaking, in that equation, the entity that acts or intervenes is not a technology company. If we think in a different paradigm, another way to think about the Cambridge Analytica incident emerges. The relationship between citizens and their government can be equated to that of a customer and a business. By substituting Facebook for the government in this comparison, a different narrative emerges in which Facebook acted to protect its "customers" after they were harmed by Cambridge Analytica. In the following section, several models will be proposed to see if any of these can serve as a frame for the perspective from Facebook as a

business, after which a determination is made whether Facebook protected its users from further harm post-Cambridge Analytica.

Smith and Huntsman, scholars in public administration, discuss an alternative to the "customer-centered public administration" model in an "exploratory field study", in which citizens are not viewed as "shop-walking proprietors" who "buy" a type of government, but as investors in a business (309–10). In this model, citizens invest their time and resources in society and expect to receive value in return. Where traditionally, the media encourages citizens to think about the cost of government, the "value perspective" seeks to map out the gains and benefits citizens receive from their investment in said government (Smith and Huntsman 310).

Traditionally, there are two ways to look at the customer-government model. The first is the customer model, in which citizens are regarded as "consumers of government services." This model borrows from the total quality management movement, a prominent private sector methodology to improve overall level of service. The government is the "producer, manufacturer, and deliverer" of these services, along with all the responsibilities that come with that. These responsibilities mean that they should "act as owners do in private business," which meant they should listen to their customers, improve the convenience of their service, and expand programs where possible (Smith and Huntsman 311). This ideology of running government services was supported by President Clinton in 1993 by means of an executive order, in which he ordered federal agencies to survey customers, set service level standards, and further develop "customer complaint systems" (Smith and Huntsman 311).

The owner model is the second method outlined by Smith and Huntsman, in which citizens are assumed to be more proactive in their role as "owners of government" (311–12). In this comparison, public servants are regarded as the administrators of a "public enterprise of

business." Citizens are presumed to work for this business and provide it with the capital required to run it. Because of this relationship, "citizen-owners" are permitted to inquire about the state of their business and look into "the affairs of their agents" whenever they please (Smith and Huntsman 311). This way of thinking empowers citizens to take an active role, both as owners and supervisors, in checking up on the quality of government services. For instance, according to advocates for this model, citizens should "inspect police records, note patent violations, […] check on play space, and even use personal vacation time to compare urban services." However, this model is not practical in theory. The owner of a business is often someone with the sole responsibility for the welfare of a given enterprise, and this responsibility cannot be divided up among a large group of citizens (Smith and Huntsman 312). Ownership rights for citizens, then, remain a theoretical concept with little basis in practice.

Smith and Huntsman propose a third model that they call the value model, based on the fortes of the customer and owner models. In this model, citizens and the government are focused on the common goal of "incrementing value" for all. In this way of thinking, citizens are not owners or customers, but rather shareholders of a "community enterprise," and the government is a trustee, charged with managing the enterprise's "assets, programs, and services" (Smith and Huntsman 313). According to the researchers, that trustee status serves an important meaning, as it implies that the task of governing, or rather the "community enterprise," is something that is entrusted to the people working as public servants. This means that "character and moral responsibility" are, in a way, more important than being an effective administrator, as government officials cannot do their job if their character is compromised, even though they might otherwise be good at their job (Smith and Huntsman 313).

Citizens and the government come together to "create incremental value" in numerous ways. The first is to determine what areas of policy are most important to citizens, and then to increase the worth of these areas through the services facilitated by the government. Second, the government should make sure money gets invested in the "capital asset base" of the community, by building public services, parks, and other facilities (Smith and Huntsman 313). One example of an investment like this is the U.S. national park system, which is maintained by the federal government so that American citizens can enjoy them at will. Citizens are not expected to invest in every part of the government as shareholders, but only where they can expect a return on their investment.

If we take the value model of administration and apply it to Facebook, it could be argued that it is, to an extent, applicable to the relationship between its users and the company. Users have an interest in providing their data to Facebook, as they want to use it to share that data with their friends. They could use it to share photos, keep up with their favorite artists, or engage in political discussion in a Facebook group. For some users, the advertisements they see might even play a role, as Facebook offers personalized advertising pertaining to your specific likes and dislikes. For Facebook, maintaining a good relationship with its users so that they keep providing the platform with useful data is paramount. The company makes its money in various ways, but primarily by using that data to show personalized advertising.

When we establish that Facebook and its users rely on each other to further their own goals, it is then in Facebook's interest to protect its users when they undergo harm (that is, when the harm principle is triggered). In practice, the company did take some action to repair some of the damage after the Cambridge Analytica incident became public knowledge. Apps that worked similarly to the app professor Kogan originally used were blocked from obtaining information in

the same way. The company promised it would implement the European General Data Protection Regulation worldwide, giving users more control over and insight in what data Facebook collects on them. Furthermore, as said before, the company rewrote its terms and conditions so that it is easier for users to understand what Facebook does with their data and how the company makes its money (European Commission).

In the eyes of regulators on both sides of the Atlantic, Facebook did not do enough to protect its users. The Federal Trade Commission voted 3-2 (the votes in favor were Republican, while the votes against were Democrat) on a five billion dollar fine for Facebook, specifically for the privacy violations committed by the Cambridge Analytica scandal. However, many people disagree with the settlement. Even though the fine is the highest ever given to any company for a privacy violation, it is not proportional to Facebook's revenue numbers that are much higher than this fine. In the settlement agreement, Facebook pledged to review and improve the ways in which it deals with data, but the FTC did not stop the company from sharing user data with third parties, which means that another Cambridge Analytica incident is technically still possible (Wong, "Facebook Is Fined $5bn").

The "symbiotic" relationship between Facebook and its users is represented differently in another context. A social sciences initiative was started by the company right around the time the Cambridge Analytica incident became public knowledge, labeled the "Social Media and Democracy" program. Academics will be able to gain access to data from Facebook under strict circumstances, under terms governed by "tripartite cooperation among academics, the private sector and government" (Igo, "We Are All Research Subjects Now"). Before, potential researchers would resort to either unsanctioned access or workarounds in order to gain access to bulk data for academic purposes. Both professor Kogan's app and the Tastes, Ties, and Time

study are good examples of this. Now, scholars will be able to do research on electoral manipulation, the effects of social media, and fake news in more detail than ever before, producing "findings that improve everybody's lives" (Igo, "We Are All Research Subjects Now").

However, as Igo points out, promises of scientific integrity ring hollow when the already-fragile reputation of a company like Facebook is at stake. In order to keep itself separate from studies that are to be performed with its data, Facebook has pledged it will not interfere in any way after it has delivered the requested data to researchers. However, as Zimmer pointed out, even "good faith-attempts" based on terms and conditions regarding what can be done with the data, mistakes can still be made (Zimmer 313).

Another blatant integrity issue is the protection of the anonymity of the people involved in Facebook's datasets. Examples of how this can go wrong are plenty, both in "debates from the 1960s about research subjects' right to dignity and privacy" to more recent examples, such as the 2008 T3 study (Igo, "We Are All Research Subjects Now"). As Igo points out, in an age of extremely sophisticated forensic techniques for social media (much more so than in 2008), how can the anonymity of subjects be guaranteed? Researchers will always do everything they can to make sure their datasets are anonymized, but even as we move toward an age of even more computing power, it will become extremely difficult to ensure that the data remains anonymous in the future.

The second issue is that Facebook's datasets are not based on willing research subjects that have signed anything resembling "informed consent," but on users on the platform that correspond with the types of data requested by scientists (Igo, "We Are All Research Subjects Now"). Some critics argue that because the data is anonymized before any scholar gets to see it,

the subjects are not recognized as traditional research subjects, and the rules of "informed consent" do not apply. On the other hand, the discussion surrounding subjects' rights in the twentieth century could not "resolve every ethical quandary" either (Igo, "We Are All Research Subjects Now"). This makes it even more imperative to reopen the conversation. In Igo's words, "a bold research agenda […] can swiftly be derailed by ethical missteps."

Conclusion

This thesis aimed to analyze the relationship between John Stuart Mill's harm principle and the Cambridge Analytica data breach that affected tens of millions of Facebook users. Because the harm principle governs the relationship between a government-like entity and individual citizens, it does not lend itself precisely to the situation surrounding Cambridge Analytica. By framing this question within a "customer-centered public administration model," the situation does allow for analysis, because this approach places Facebook in the position of "government" in the harm principle equation. Specifically, the "value model" looked at the interaction between Facebook and its users as one of mutual benefit, where Facebook needs to keep its users satisfied so they will continue to use the platform.

This methodology let us test the Cambridge Analytica scandal from different scholarly perspectives and to see whether the situation triggers the harm principle or not. As it turns out, the distinctions in the various interpretations of what the harm principle means affect whether the harm principle is triggered. This appears to depend on what academic discipline the subject is approached from. Where philosophy scholars appear to leave more room for nuance in their interpretations, the harm principle has "collapsed" in on itself according to a legal scholar, removing the threshold altogether. An information privacy scholar, on the other hand, clearly believed that mismanaging data violates the harm principle. Further analysis of the differences in dealing with Mill's harm principle are beyond the scope of this thesis, but even in this limited study, the variations in nuance were striking.

The privacy debate in the United States has never been more complex than as it is right now. New technologies are meeting established constitutional law, and people are finding that the two are not yet entirely compatible. Many questions regarding these new developments still

remain unanswered. Even though some of these landmark cases deal with similar questions regarding new technologies, there is still uncharted territory left to be explored by the courts. For instance, regulations surrounding aerial drones for consumers touch upon many legislative aspects that are in place today, but need their own judicial response, to clear up confusion and to set proper expectations for consumers.

Many older court cases are still relevant today, including cases that go back as far as the nineteenth century. Cases like *Ex parte Jackson* (1877) laid the foundation for laws that govern electronic communication today and serves to illustrate that the Supreme Court often reaffirms societal tendencies or institutional attitudes by means of a case. "The Right to Privacy," although over a hundred years old at this point, outlines a fundamental right that plays an important role in modern discussions about privacy, both in an online and offline context.

When looking at Supreme Court cases, it is important to be mindful of the interdisciplinary nature of some of the cases that were discussed. When considering *Roe v. Wade*, for instance, many people would think about the pro-life vs. pro-choice debate, without realizing that it was also an important case for privacy. That case in particular is worthy of further study, due to those broad implications.

Facebook has had a troubled relationship with privacy as a concept. Where the company embraced its death in the early years of its existence, Mark Zuckerberg has now accepted that privacy is something his customers want to have control over. It is now his company's "main focus," which is not surprising in a way. After the Cambridge Analytica incident, Zuckerberg was apologetic and promised he would do better in the future, as he felt he was responsible himself, as the founder of Facebook. That shift in attitude is surprising, as the company has had multiple incidents with regards to privacy in the past. Most of these incidents can be summarized

as problems in which users posted content to the network, without realizing that their posts were visible to the public, either by user error due to an update or because a problem with the website revealed their posts.

But not all privacy violations can be blamed on Facebook, as users themselves can also be blamed. Either researchers do not anonymize the data of their subjects well enough when distributing it for research purposes, or users simply do not read the terms and conditions they are agreeing to when signing up for a new service. Studies show that less than forty percent of all users read user agreements, so-called "click-wrap agreements," which potentially means they open themselves up to lawsuits or worse if they do not abide by that agreement. In the specific context of Facebook, that means the company should not use their own terms and conditions as a defense to users who did not read them, which it has done in the past.

Whether Facebook's behavior will change in the future is difficult to say. Although the company has been fined by the Federal Trade Commission, many people are critical of this move. The agreement the company struck with the FTC does not preclude them from selling data to third parties in the future, which means that another Cambridge Analytica-like incident could happen again. Thanks to Facebook's new social sciences initiative, in which the company will put together datasets for sociological research, that could very well happen. After all, it would not be the first time that data collected for academic purposes ends up in the wrong hands. That is exactly what happened with professor Kogan's app and Cambridge Analytica.

Suggestions for further research

This thesis deals with the Cambridge Analytica case from the perspective of an American Studies scholar. That means that even though some of the ideas and scholars mentioned might be from outside the United States, the perspectives, attitudes, and abstract interactions discussed are inherently American. Because Facebook is operating globally, with users in just about every country, it would be worth the effort to perform a similar study on the incident in other countries. For instance, adding a European viewpoint to the discussion could result in a more transatlantic perspective on the ways in which people think about privacy and attitudes toward harm.

Such a view would also be a useful addition to the existing scholarship on privacy, as the digital aspect of that has not been explored as well as other, older fields. This particular branch of privacy will only become more relevant in the future, as more and more of our lives moves to the digital space. That does not just apply to what people do in their free time, but also to the ways in which governments interact with their citizens.

The 2002 Adam Gatt study was performed in a time with a different internet climate, and the average familiarity level with internet technology among the average user has risen significantly. Not only that, the demographics of internet users have likely changed since the original study. It could be worthwhile to do a similar survey as a comparative study to the results achieved in 2002. By doing this, researchers could gauge changes in attitudes among users to dealing with click-wrap agreements. It would also be interesting to see if users are more reluctant to leave their names and email addresses with internet companies, or if there has not been much change at all. Another interesting statistic would be to explore whether smartphones have influenced this behavior at all.

Igo lamented the partnership between Facebook and the Social Science Research Council that would permit social scientists to do research using datasets from anonymized Facebook users. Studies like this have the potential to go wrong, just like the Tastes, Ties, and Time study by Lewis et al. did. A comparison between a modern study, performed using one of the new Facebook datasets, and the T3 study could provide further insight into the process of doing research with an anonymized dataset and the pitfalls associated with it. A comparative study would then also confirm or deny Igo's concerns regarding "ethical quandaries" and "confidentiality" ("We Are All Research Subjects Now").

Works Cited

Abril, Patricia Sánchez, et al. "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee: Social Media Privacy and the Twenty-First-Century Employee." *American Business Law Journal*, vol. 49, no. 1, Mar. 2012, pp. 63–124. *DOI.org*, doi:10.1111/j.1744-1714.2011.01127.x.

Amer, Karim, and Jehane Noujaim. *The Great Hack*. Netflix, 2019. Netflix.

Bloch, Ruth H. "The American Revolution, Wife Beating, and the Emergent Value of Privacy." *Early American Studies: An Interdisciplinary Journal*, vol. 5, no. 2, 2007, pp. 223–51. *DOI.org (Crossref)*, doi:10.1353/eam.2007.0008.

Bremer, Francis J. *Puritanism: A Very Short Introduction*. Oxford University Press, 2009.

Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, 17 Mar. 2018, http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Channel 4 News. "Exposed: Undercover Secrets of Trump's Data Firm." *Channel 4 News*, https://www.channel4.com/news/exposed-undercover-secrets-of-donald-trump-data-firm-cambridge-analytica.

Constine, Josh. "WhatsApp Hits 1.5 Billion Monthly Users. $19B? Not so Bad." *TechCrunch*, http://social.techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad/.

"Constitutional Law: Supreme Court Finds Marital Privacy Immunized from State Intrusion as a Bill of Rights Periphery." *Duke Law Journal*, vol. 1966, no. 2, 1966, pp. 562–77. JSTOR, *JSTOR*, doi:10.2307/1371542.

Contiguglia, Cat. “Cambridge Analytica Shutting Down.” *POLITICO*, 2 May 2018, https://www.politico.eu/article/cambridge-analytica-shutting-down/.

Davies, Harry. “Ted Cruz Campaign Using Firm That Harvested Data On Millions Of Unwitting Facebook Users.” *The Guardian*, 11 Dec. 2015, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

Desai, Anuj C. “Wiretapping before the Wires: The Post Office and the Birth of Communications Privacy.” *Stanford Law Review*, vol. 60, no. 2, 2007, pp. 553–94. JSTOR.

European Commission. *Press Release - Facebook Changes Its Terms And Clarify Its Use Of Data For Consumers Following Discussions With The European Commission And Consumer Authorities*. https://europa.eu/rapid/press-release_IP-19-2048_en.htm.

Flavell, Julie M. “Government Interception of Letters from America and the Quest for Colonial Opinion in 1775.” *The William and Mary Quarterly*, vol. 58, no. 2, 2001, pp. 403–30. *JSTOR*, doi:10.2307/2674191.

Gatt, Adam. “Electronic Commerce - Click-Wrap Agreements.” *Computer Law & Security Review*, vol. 18, no. 6, Nov. 2002, pp. 404–10. *Crossref*, doi:10.1016/S0267-3649(02)01105-6.

Harcourt, Bernard E. “The Collapse of the Harm Principle.” *The Journal of Criminal Law and Criminology (1973-)*, vol. 90, no. 1, 1999, pp. 109–94. JSTOR, *JSTOR*, doi:10.2307/1144164.

Hill, Kashmir. “Facebook Is Giving Advertisers Access to Your Shadow Contact Information.” *Gizmodo*, https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051.

Hochstetler, Laurie. “Making Ministerial Marriage: The Social and Religious Legacy of the Dominion of New England.” *The New England Quarterly*, vol. 86, no. 3, 2013, pp. 488–99. JSTOR.

Igo, Sarah Elizabeth. *The Known Citizen: A History of Privacy in Modern America*. Kindle ed., Harvard University Press, 2018.

---. “We Are All Research Subjects Now.” *The Chronicle of Higher Education*, Oct. 2018. *The Chronicle of Higher Education*, https://www.chronicle.com/article/We-Are-All-Research-Subjects/244705.

Isaac, Mike, and Sheera Frenkel. “Facebook Security Breach Exposes Accounts of 50 Million Users.” *The New York Times*, 23 Oct. 2018. *NYTimes.com*, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

Johnson, Bobbie. “Privacy No Longer a Social Norm, Says Facebook Founder.” *The Guardian*, 11 Jan. 2010, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

Johnson, Richard R. “‘Parliamentary Egotisms’: The Clash of Legislatures in the Making of the American Revolution.” *The Journal of American History*, vol. 74, no. 2, 1987, pp. 338–62. JSTOR, *JSTOR*, doi:10.2307/1900026.

Kakaes, Konstantin. “Drones Can Photograph Almost Anything. But Should They?” *Columbia Journalism Review*, 21 Apr. 2016, https://www.cjr.org/the_feature/drones_can_photograph_almost_anything_but_should_they.php.

Kasper, Debbie V. S. “The Evolution (Or Devolution) of Privacy.” *Sociological Forum*, vol. 20, no. 1, 2005, pp. 69–92. JSTOR, *JSTOR*, doi:10.1007/s11206-005-1898-z.

Kelling, George L., and James Q. Wilson. “Broken Windows.” *The Atlantic*, Mar. 1982, https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/.

Lewis, Kevin, et al. “Tastes, Ties, and Time: A New Social Network Dataset Using Facebook.Com.” *Social Networks*, vol. 30, no. 4, Oct. 2008, pp. 330–42. *Crossref*, doi:10.1016/j.socnet.2008.07.002.

Macleod, Christopher. “John Stuart Mill.” *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Spring 2018, Metaphysics Research Lab, Stanford University, 2018. *Stanford Encyclopedia of Philosophy*, https://plato.stanford.edu/archives/spr2018/entries/mill/.

Mill, John Stuart, and John M. Robson. *Collected Works of John Stuart Mill. Vol. 18 1: Essays on Politics and Society [...]*. University of Toronto Press, 1977.

Ministerie van Algemene Zaken. *Waar moet ik aan denken als ik de voornaam voor mijn kind kies? - Rijksoverheid.nl*. 8 June 2015.

Riley, Jonathan. “Is Mill an Illiberal Utilitarian?” *Ethics*, vol. 125, no. 3, 2015, pp. 781–96. *JSTOR*, doi:10.1086/679556.

---. *The Routledge Guidebook to Mill’s On Liberty*. Routledge, 2015.

Rosenberg, Matthew, et al. “How Trump Consultants Exploited the Facebook Data of Millions.” *The New York Times*, 2 Apr. 2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Rubenfeld, Jed. “The Right of Privacy.” *Harvard Law Review*, vol. 102, no. 4, 1989, pp. 737–807. JSTOR, *JSTOR*, doi:10.2307/1341305.

Schaake, Marietje. “Beware of Tech Companies Playing Government.” *Bloomberg*, 17 Jan. 2019, https://www.bloomberg.com/opinion/articles/2019-01-17/beware-of-tech-companies-playing-government.

Schwartz, Paul M. “Property, Privacy, and Personal Data.” *Harvard Law Review*, no. 7, 2004 2003, pp. 2056–128.

Sklansky, David Alan. “Too Much Information: How Not to Think About Privacy and the Fourth Amendment.” *California Law Review*, vol. 102, no. 5, 2014, pp. 1069–121. JSTOR.

Smith, Brad. “34 Companies Stand up for Cybersecurity with a Tech Accord.” *Microsoft on the Issues*, 17 Apr. 2018, https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/.

Smith, Gerald E., and Carole A. Huntsman. “Reframing the Metaphor of the Citizen-Government Relationship: A Value-Centered Perspective.” *Public Administration Review*, vol. 57, no. 4, 1997, pp. 309–18. JSTOR, *JSTOR*, doi:10.2307/977312.

Sutherland, Arthur E. “Privacy in Connecticut.” *Michigan Law Review*, vol. 64, no. 2, 1965, pp. 283–88. JSTOR, *JSTOR*, doi:10.2307/1287070.

The Guardian. “Facebook Reveals It Gave 61 Companies Access To Widely Blocked User Data.” *The Guardian*, 3 July 2018, https://www.theguardian.com/technology/2018/jul/02/facebook-user-data-access-companies-privacy.

Turner, Piers Norris. “‘Harm’ and Mill’s Harm Principle.” *Ethics*, vol. 124, no. 2, Jan. 2014, pp. 299–326. *Crossref*, doi:10.1086/673436.

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review*, vol. 4, no. 5, 1890, pp. 193–220. JSTOR, *JSTOR*, doi:10.2307/1321160.

Watson, Chloe. “The Key Moments From Mark Zuckerberg’s Testimony To Congress.” *The Guardian*, 11 Apr. 2018, https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments.

Whitman, James Q. “The Two Western Cultures of Privacy: Dignity versus Liberty.” *The Yale Law Journal*, vol. 113, no. 6, Apr. 2004, pp. 1151–221. *Crossref*, doi:10.2307/4135723.

Wong, Julia Carrie. “Facebook to Be Fined $5bn for Cambridge Analytica Privacy Violations – Reports.” *The Guardian*, 12 July 2019, https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations.

---. “Zuckerberg Says Facebook Is Pivoting to Privacy after Year of Controversies.” *The Guardian*, 6 Mar. 2019, https://www.theguardian.com/technology/2019/mar/06/mark-zuckerberg-facebook-privacy-vision.

Ziegler, Mary. “The Framing of a Right to Choose: Roe v. Wade and the Changing Debate on Abortion Law.” *Law and History Review*, vol. 27, no. 2, 2009, pp. 281–330. JSTOR.

Zimmer, Michael. “‘But the Data Is Already Public’: On the Ethics of Research in Facebook.” *Ethics and Information Technology*, vol. 12, no. 4, Dec. 2010, pp. 313–25. *Crossref*, doi:10.1007/s10676-010-9227-5.