**Privacy and the Ubiquitous Nature of Modern Technology**

Martin J. Adamian, J.D., Ph.D.

California State University, Los Angeles

Gretchen Lawrie, J.D., L.L.M.

California State University, Los Angeles

Prepared for the Western Political Science Association 2019 Annual Conference

in San Diego, California, April 18 - 20, 2019

Abstract:

Instead of a single, comprehensive federal privacy law, Congress has enacted a patchwork of laws recognizing and protecting individual’s privacy with some laws protecting categories of personal information and other ones applying to the use of personal information. These laws exist at the state, federal, and international level and have implications for individuals, as well as corporations and governments. The need for corporations to be able to access large markets, such as Europe, California and others more interested in protecting individual privacy, has the potential to ensure that even the most reluctant players will be forced to protect privacy. This paper will look at the complicated web of privacy laws and their repercussions for individuals and corporations. The ways we respond to new threats to privacy generated by the ubiquitous nature of modern technology and social media has the potential to significantly alter the ability of individuals and corporations to thrive.

On April 14, 2016, the European Parliament and Council of the European Union passed the General Data Protection Regulation[[1]](#footnote-1) (GDPR), which went into effect on May 25, 2018. This new European Union (EU) law addresses data protection and privacy for all individuals within the EU and the European economic area. For many, privacy protections are much needed and overdue as we increasingly trade our privacy for the convenience of modern technology. In this regard, many see the need for strict laws that provide individuals with greater power to control information about themselves. Certainly, this is important to Europeans and has been reflected in the GDPR, but it is also true for Americans. Yet, to date there is no coherent and comprehensive privacy laws in the United States (US). Instead, the US has opted for a patchwork of federal and state, constitutional and statutory privacy laws that emphasize the interests of corporations, often at the expense of individuals. In addition, many see an irreconcilable conflict between the right to privacy as articulated in the GDPR and the fundamental right to freedom of speech protected by the First Amendment to the US Constitution. As a result, a fundamental rift has developed between Europe and the US in regard to privacy protections and the desirability of a one-size-fits-all solution.

This paper starts from the premise that privacy is important, and worth protecting through international and regional laws, as well as through the domestic law of states. However, important questions remain about the extent to which Europe and/or California maybe able to impose a specific understanding of privacy on the rest of the globe. As we will see, these debates are currently playing themselves out in regard to the extraterritorial aspirations of the GDPR, as well as the current US federal privacy proposals. We stand on a precipice as modern technology continues to blur the line between public and private, and our laws struggle to keep pace. While it is tempting to pursue rigorous international and regional legal agreements, it is also important to recognize the privacy is a complex social practice that varies over time and space. The difference between Europeans and Americans in regard to privacy is just one example of the many ways in which individuals’ expectations of privacy are shaped by culture, history, architecture, and technology. The question remains, can the European model, or any other comprehensive privacy laws be constructed in such a way that recognizes these differences and provides the flexibility to respond to the ever-changing world in which we live.

**Privacy Laws in Europe**

As a result of differences in history, culture, and architecture, Europeans have a much different understanding of the need for privacy than others, particularly those in the US.[[2]](#footnote-2) In Europe, privacy is viewed as a fundamental right and “expressed in omnibus laws that regulate the public and private sectors…”[[3]](#footnote-3) The European Convention on Human Rights (ECHR), which became enforceable in 1953, provides the right of privacy and the protection of the freedom of expression. Article 8 of the ECHR states that “Everyone has the right to respect for his private life, his home and his correspondence’’ and “[t]here shall be no interference by a public authority with the exercise of this right…” Further, it is worth noting that the ECHR anticipated the potential for this right to conflict with other rights, including the freedom of expression. In this regard, Article 10 provides that “[e]veryone has the right to freedom of expression…” However, the exercise of this freedom can “…be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society… for preventing the disclosure of information received in confidence…”[[4]](#footnote-4)

Besides individuals having a general right to privacy in Europe, they also have the right to privacy of their personal data. In 1995, the European Parliament and the European Council passed the Data Protection Directive[[5]](#footnote-5) (DPD) with the objective for member states to “… protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.”[[6]](#footnote-6) The DPD set out standards for the protection of data within the EU and required member states to enact their own national laws based on these standards.[[7]](#footnote-7)

The DPD applied to the processing of personal data where: 1) the processing was carried out by a controller[[8]](#footnote-8) established in the EU; or 2) the processing was carried out by a controller outside the EU on equipment located in the EU, unless the equipment was used only for purposes of transit through the EU.[[9]](#footnote-9) The DPD prohibited the transfer of personal data to countries outside of the EU that did not have “an adequate level of protection.”[[10]](#footnote-10) However, data could be transferred to a country that did not have an adequate level of protection, if the country’s laws were sufficient or the country had entered into agreements to protect “…the private lives and basic freedoms and rights of individuals.”[[11]](#footnote-11)

In order to modernize and harmonize the EU’s privacy laws and have “a one-stop-shop mechanism” to ensure a uniform and consistent application of data privacy laws in the EU member states, the Council of the European Union and the European Parliament, in April 2016, enacted the GDPR to replace the DPD, which became effective in May 2018.[[12]](#footnote-12) The GDPR replaced “28 different sets of national privacy laws” that were enacted by EU members in order to implement the DPD with one data privacy law applicable to all member states.[[13]](#footnote-13) The GDPR is intended to protect the “… fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.” [[14]](#footnote-14) Also, it is meant to “…strengthen the protection of the individual’s right to personal data protection, reflecting the nature of data protection as a fundamental right for the European Union.”[[15]](#footnote-15)

The GDPR applies to a person or entity, such as a corporation, that is established in the EU and controls or processes personal data inside and outside the jurisidicational boundaries of the EU.[[16]](#footnote-16) The GDPR uses the terms data controller and data processor. A data controller is natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes or interests of processing personal data. A data processor is a natural or legal person, public authority, agency or other body which processes data on behalf of the data controller. The GDPR also applies to a person or entity that is not established in the EU, but processes data related to: 1) the offering of goods or services to individuals in the EU, even if a payment is not required; or 2) monitoring the behavior of these individuals, if the behavior occurs in the EU.[[17]](#footnote-17) However, the GDPR does not apply to processing of personal data: 1) by an individual in the course of a purely personal or household activity; and 2) by competent authorities to prevent, investigate, detect, or prosecute criminal offences or execute criminal penalties.[[18]](#footnote-18)

The GDPR reflects the emphasis on the individual in European privacy laws. Under the GDPR, individuals’ personal data cannot be collected or processed, unless they have given their explicit consent, which they can withdraw at any time.[[19]](#footnote-19) However, their information can be collected or processed without their consent in circumstances, such as complying with a legal obligation, protecting individuals’ vital interests, or performing a task carried out in the public interest.[[20]](#footnote-20) The GDPR also gives individuals the right to access and obtain copies of their personal data and to object to the collection and/or processing of their personal information. They also have the right to request to have inaccurate personal data corrected and incomplete information completed.[[21]](#footnote-21) Individuals also have the right to request that their personal information be deleted in certain circumstances, such as their personal data is no longer necessary in relation to the purposes for which it was collected, they withdraw their consent or objects to the processing of their data, or their data had been unlawfully processed.[[22]](#footnote-22) Upon request, individuals’ personal information must be permanently removed and deleted. However, personal data cannot be deleted for various reasons including where the data is necessary for exercising the right to freedom of expression or for public health, statistical, scientific, or historical research purposes.[[23]](#footnote-23) If an individual’s rights under the GDPR are infringed upon or violated, national regulators can assess a fine of up to 4 percent of a company’s or other entity’s total world-wide annual revenue for the preceding financial year or 20 million euros, whichever is higher.[[24]](#footnote-24) As we will see, the US does not provide the same level of protections for individuals, instead emphasizing corporations and business interests.

**Privacy Laws in the United States - Federal**

In the United States, there is patchwork of federal and state constitutional and statutory privacy laws, instead of a single comprehensive law. Although it is generally agreed that Louis D. Brandeis and Samuel D. Warren were the first to discuss the existence of a right to privacy in their 1890 law review article published in the *Harvard Law Review*,[[25]](#footnote-25) the full recognition of the right to privacy came much later. In 1960, Richard Prosser wrote a *California Law Review* article titled “Privacy,” which was subsequently entered into the Second Restatement of Torts at §§ 652A-652I (1977).[[26]](#footnote-26) Prosser mentions the Brandeis and Warren article and suggests that it was the first in a series of law review articles on the right to privacy, most of which agreed with Brandeis and Warren and supported the existence of a right to privacy. Prosser goes on to discuss the early cases addressing such a right.

By 1960 there were already more than 300 privacy cases in the books, leading Prosser to suggest that the “holes in the jigsaw puzzle have been largely filled in, and some rather in definite conclusions are possible.”[[27]](#footnote-27) He concludes that there is not just one common law tort related to a right to privacy, but a complex of four. “The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, up which are tied together by the common name, but otherwise have almost nothing in common.”[[28]](#footnote-28) He went on to discuss the following four torts:

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff and a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.[[29]](#footnote-29)

These categories of privacy have been embraced by the courts in different jurisdictions to varying degrees, and Prosser provides a detailed discussion of the relevant cases of the day.[[30]](#footnote-30) Some of these laws have been codified in state and federal statutes, while others rely on case law to protect individuals from invasions of privacy by others. However, given the rich history of privacy in common law cited by many legal scholars and jurists, many questioned the existence of a constitutional right to privacy that would protect individuals from invasion by government.

The U.S. Constitution does not explicitly guarantee or protect the right to privacy and Congress has not enacted laws providing a general right to privacy. However, the Court has recognized that the right to privacy is implicitly derived from fundamental constitutional guarantees that create zones of privacy.[[31]](#footnote-31) In *Griswold vs. Connecticut*, the Court discussed the existence of a number of rights that are not specifically stated in the Constitution or the Bill of Rights and that these rights are consistent with the spirit of the Constitution and are necessary in order to secure existing rights. [[32]](#footnote-32) Further, these rights, referred to as the penumbra of rights, are “formed by emanations from those guarantees that help give them life and substance” and these “[v]arious guarantees create zones of privacy.”[[33]](#footnote-33) For example, according to the Court, the Fourth Amendment’s “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” creates a zone of privacy that protects individuals from invasion by the government. The Court found that *Griswold* concerned a relationship lying within the zone of privacy created by several fundamental constitutional guarantees. It held that the Connecticut law forbidding the use of contraceptives violated the right of “marital privacy which is within the penumbra of specific guarantees of the Bill of Rights,” and therefore the law was unconstitutional.

Since *Griswold*, Congress has enacted a patchwork of laws that govern the use and protection of an individual’s privacy for specific purposes, in certain situations, or by certain sectors or types of entities. For privacy of individuals’ personal data, Congress has enacted “industry-specific laws that regulate the collection and protection of sensitive personal information.”[[34]](#footnote-34) For example, in 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act, known as the Wiretap Act, prohibiting, except in certain circumstances, the unauthorized and/or nonconsensual interception of oral and wire communications by government agencies without obtaining prior judicial authorization.[[35]](#footnote-35) However, under 18 U.S. Code § 2518(7), prior judicial authorization is not required, if an investigative or law enforcement officer reasonably determines that an emergency situation exists that involves immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime that requires interception of wire and oral communications before judicial approval can be obtained.

In 1986, the Electronic Communications Privacy Act (ECPA) extended the Wiretap Act to include interception of computer and other digital and electronic communications, such as email, and also provided protection of wire, oral, and electronic communications when they are being made, are in transit, or stored on computers. As part of the ECPA, Congress enacted the Stored Communications Act of 1986 (SCA), which applies to providers of electronic communication services (ECS) and remote computing services (RCS). Providers of ECS to the public are prohibited from knowingly disclosing to any person or entity the contents of a communication while in electronic storage.[[36]](#footnote-36) RCS providers provide computer storage or processing services by means of an electronic communication system. Like ECS providers, providers of RCS to the public are prohibited from knowingly disclosing the contents of a communication which is carried or maintained by the RCS providers.[[37]](#footnote-37)

Public providers of ECS or RCS are also prohibited from disclosing a customer’s information or record to any government entity. However, a customer’s information can be disclosed in several situations, such as when the customer has consented to the disclosure. Also, a customer’s information can be disclosed to any person, but not to a government entity, unless the provider believes in good faith that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.[[38]](#footnote-38) Under the SCA, a government entity can obtain access to non-content information, such as a customer’s name, address, or means of payment, by obtaining a warrant or an administrative subpoena.[[39]](#footnote-39)

The Financial Services Modernization Act of 1999, referred to as the Gramm-Leach-Bliley Act (GLBA), requires financial institutions to respect their customers’ privacy and to protect the security and confidentiality of their nonpublic personal information.[[40]](#footnote-40) Financial institutions covered by the GLBA are not to disclose their customers’ nonpublic personal information to unaffiliated third parties unless they provide written or electronic privacy notices to their customers and inform them that they can opt out of having their information shared with third parties.[[41]](#footnote-41) However, financial institutions can disclose their customers’ nonpublic personal information to third parties for purposes, such as marketing the financial institutions own products and services.[[42]](#footnote-42)

The administration and enforcement of the numerous and separate privacy laws is carried out by several different federal agencies, rather than by one agency. One of the agencies is the Federal Trade Commission (FTC), which has described itself as “…the nation’s primary privacy and data security enforcer,” administers and/or enforces several privacy related laws, such the Children’s Online Privacy Act, the Video Privacy Protection Act, and the Gramm-Leach-Bliley Act.[[43]](#footnote-43) Also, using its authority under section 5 of the Federal Trade Commission Act of 1914 (FTC Act) to prohibit “unfair or deceptive acts or practices in or affecting commerce,” the FTC has taken legal actions against organizations that “have violated consumers’ privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury.”[[44]](#footnote-44)

In its first internet privacy case in 1998, the FTC alleged that the website, GeoCities, misrepresented that its members’ personal identifying information, such as occupation, age, and email addresses, would only be used to provide them with specific advertising offers, products, or services that they had requested and would not be released to anyone without the members’ requests. However, GeoCities had disclosed its members’ information to third parties, who used it to target members for solicitations beyond those agreed to by the members. Under a settlement agreement, GeoCities agreed to post a clear and prominent privacy notice telling consumers what information was being collected and for what purpose, to whom it would be disclosed to, and how they could access and remove their information.[[45]](#footnote-45)

Although prior to 2015 the FTC had asserted jurisdiction over the privacy practices of both internet service and content providers, in 2015, the Federal Communications Commission (FCC) asserted primary oversight over internet service providers by classifying broadband as a telecommunication service, rather than an information service, resulting in internet service providers being considered telecommunications carriers subject to the Communications Act and the FCC’s, not the FTC’s jurisdiction. Then, in 2016, the FCC promulgated privacy regulations specific to internet service providers. But prior to going into effect in 2018, Congress in 2017 repealed the regulations and the FCC re-classified broadband as an information service, thus effectively transferring jurisdiction over internet privacy back to the FTC.[[46]](#footnote-46)

**Privacy Laws in the United States - State**

Most states recognize the right to privacy and have enacted laws protecting an individual’s right to privacy with some states enacting laws protecting an individual’s data.[[47]](#footnote-47) For example, in 1972, California voters approved amending the state of California’s Constitution to include the right of privacy as an inalienable right. As amended, Article 1, section 1 of California’s Constitution provides that: “[a]ll people are by nature free and independent and have inalienable rights. Among these are… pursuing and obtaining safety, happiness, and privacy.” Besides recognizing a right to privacy, California and other states have either passed or considered laws protecting personal data, such as California’s Online Privacy Protection Act and Consumer Data Privacy Act.[[48]](#footnote-48)

California’s Online Privacy Protection Act (OPPA) requires individuals and entities that collect California residents’ personally identifiable information through internet web sites or online services for commercial purposes to post and comply with a privacy policy. Operators are required to disclose in their privacy policies the categories of personally identifiable information they collect on users and the third parties that information is shared with. Also, in their policies, operators must state how they respond to users’ Do Not Track requests and disclose that third parties may be tracking users’ activities on the web site.[[49]](#footnote-49)

In 2018, California enacted the Consumer Data Privacy Act (CDPA), effective in 2020, which gives individual Californian consumers several rights, including the right to *opt out* of a business selling their personal information to a third parties and the right to request a business to delete their personal information. Consumers can also request a business to disclose the categories and specific personal information it has collected about them, the source of the information, and the purpose for collecting their information.[[50]](#footnote-50) Further, businesses are prohibited from selling the personal information of consumers who are under the age of 16, unless the consumer is between 13 and 16 years of age and gives their consent or the parent or guardian of a consumer younger than 13 gives their consent.[[51]](#footnote-51) The CDPA applies to any business operating in California that collects consumers’ personal information and has either annual gross revenue exceeding $25 million, receives or discloses the personal data of 50,000 more California residents annually, or 50 percent of their annual revenue is from selling California residents’ personal information. The CDPA also applies to these businesses’ affiliates with whom they share a name, servicemark, or trademark.[[52]](#footnote-52) Businesses can be fined up to $2,500 for each violation or $7,000 for each intentional violation of the CDPA.[[53]](#footnote-53)

It is not uncommon for states, such as California, to impact the development of laws outside of that states jurisdiction. The “California Effect” refers to the spread of laws and regulations outside of the originating jurisdiction that influences other states, nations, and industries to conform with rules of the more or even the most restrictive state.[[54]](#footnote-54) The term comes from the impact the state of California had and continues to have on environmental and consumer regulatory standards for all other states,” the United States, and even other nations for.[[55]](#footnote-55) For example, after the enactment of Clear Act of 1970, which allowed the federal and state governments to enact rules to limit emissions, California enacted stricter environmental regulations than the federal standard. In order for auto companies to market and sell within California, they adopted California’s stricter, not the national emission standard. Also, California has had and continues to have an effect on protecting consumers’ privacy on the internet. For example, in 1998, 14 percent of internet websites posted privacy policy notices, but after California passed the OPPA in 2003, by 2011, 97 percent of websites had privacy policies.[[56]](#footnote-56) Despite the California Effect, under the doctrine of preemption, California and other states cannot promulgate privacy and other laws that are “inconsistent” with US federal laws without “explicit waiver” from the federal in the form of Congressional laws or court decisions.[[57]](#footnote-57) For example, as discussed below, some proposed Congressional internet privacy bills provide for preempting states’ internet privacy laws, and other ones do not.

It is worth noting that the California Effect is not limited to one state influencing the United States or other states, but one country can “externalize its regulations on other countries.” This is referred to as the “Brussels Effect,” recognizing that many rules and regulations that have originated in Brussels have “penetrated many aspects of economic life within and outside of Europe.”[[58]](#footnote-58) The Brussels Effect has been described as “[u]nilateral regulatory globalization” that develops when “a law of one jurisdiction migrates into another” without “the former actively imposing it or the latter willingly adopting it.”[[59]](#footnote-59) Like the state of California, because of the Brussels Effect, Europe has been able to have a “tangible impact on the everyday lives of citizens around the world” by setting “the global rules across a range of areas,” such as food, chemicals, individual privacy, and the internet.[[60]](#footnote-60) This raises some interesting questions of jurisdiction regarding the reach and influence of existing privacy laws.

**Jurisdiction**

Given the complexity and overlapping jurisdiction of international, regional, and domestic law, it is extremely difficult for an individual or a corporation to be able to navigate privacy law. This begs the question, is the move towards a single global privacy regime more desirable. Not everyone agrees. In the United States, fears remain regarding the extent to which the right to be forgotten might conflict with the First Amendment to the United States Constitution. Questions about the reach and legitimacy of the extra territorial jurisdictional provisions in the new European privacy laws have many concerned.

The new European privacy laws extend an already rigorous system of protections to a greater volume of activity, covering more individuals by providing higher penalties and additional mechanisms of the enforcement. Fines can amount to as much as 4 percent of a company’s global revenues. The GDPR also creates a new and powerful pan-European privacy regulatory agency. Together the new law is more aggressive and more explicitly seeks to spread a specific understanding of the right to privacy to a greater portion of the globe. Of course, European corporations must comply, but more interesting and controversial questions arise for companies operating outside of the borders of Europe. In the past, corporations could structure their activities to avoid EU jurisdiction. This appears to be much more difficult under the new law and legitimate questions remain as to whether this is a good thing or not.

Serious questions remain regarding whether any EU law can properly have extraterritorial effect outside the boundaries of Europe. There are long-standing legal rules on international jurisdiction that must be satisfied before regulatory agencies and courts can exercise jurisdiction over distant subjects. It appears that pure US media companies would have persuasive arguments against the jurisdiction of EU regulatory authorities and courts to enter orders against them, and a strong argument against the enforcement of such orders or subsequent fines.[[61]](#footnote-61) However, despite legal considerations there are significant reputational and practical issues that arise from resisting an order under the GDPR that companies will need to take into consideration.

Prior to the adoption of the GDPR, each EU member country implemented its own data privacy laws under the directive. The result was a patchwork of slightly divergent privacy protections in which companies could strategically select their country of affiliation based on the strength of their privacy laws. In this regard, the regulation sought to “harmoni[ze]” privacy laws in the EU by providing the consistent strong data protection for individuals across the EU. It also broadens the jurisdictional reach by covering data controllers and processors outside the EU if they offer goods and services to or monitor the behavior of EU data subjects. Further, these terms are all defined broadly to cover anything and everything.

Under international law there are several traditionally recognized bases for asserting jurisdiction, including the:

1. territoriality principle,
2. the nationality principle,
3. the passive personality principle
4. the protective principle, and
5. the universality principle.[[62]](#footnote-62)

With regard to our online conduct, states have also increasingly exercise jurisdiction under variations of these principles such as the objective territoriality test and the effects doctrine.[[63]](#footnote-63) In order to determine there applicability to issues of internet privacy, these principles will be discussed below.

***Territoriality and Nationality***

The territoriality and nationality principles are commonly invoked to permit states to assert jurisdiction over what happens within their borders as well as over acts committed by individuals and organizations of the state’s nationality even if those tasks take place outside the states physical territory.[[64]](#footnote-64) The “Objective territoriality principle,” is a variation of the traditional territoriality concept and permits a state to assert jurisdiction over acts that were initiated abroad but completed within a state’s territory, as well as where “a constitutive element of the conduct occurred” in the state.[[65]](#footnote-65) The jurisdictional test in the Directive appears to be a manifestation of the objective territoriality principle because it allows European regulators to assert jurisdiction over foreign websites or online service providers based solely on their use of equipment or the location of servers within the EU.[[66]](#footnote-66) But the GDPR goes further.

***Passive Personality and the Protective Principle***

States can also assert jurisdiction for acts committed against their own citizens by foreigners. The passive personality principle permits states to exercise authority based on their connection to the victim of illegal conduct.[[67]](#footnote-67) This basis for jurisdiction has ordinarily been limited to serious crimes, such as terrorist attacks or assassinations, and not ordinary torts or misdemeanors.[[68]](#footnote-68) It occasionally has also been applied in the civil law context.[[69]](#footnote-69) The protective principle extends this idea to allow the state to protect itself rather than its citizens from harmful acts inflicted outside of its territory.[[70]](#footnote-70)

***The Effects Doctrine***

Under the so called “the Effects doctrine,” states can assert jurisdiction based on the fact that conduct taking place entirely outside of the state has substantial effects within the state.[[71]](#footnote-71) The concept is closely related to the objective territoriality idea, but it does not require that any element of the conduct being regulated actually take place within the territory of the state. The effects doctrine is generally regarded as the most controversial basis upon which to assert jurisdiction under international law.[[72]](#footnote-72) But despite criticism, it has become widely used with regard to the conduct over the Internet.[[73]](#footnote-73) And seems to be the closest to the basis of jurisdiction relied on by the GDPR.

**Reasonableness Analysis in international jurisdiction**

The fact that conduct or activity falls under one of these bases for jurisdiction is not the end of the analysis. There is a presumption in international law that the party seeking to assert jurisdiction has to further prove why it is reasonable to exercise extra territorial jurisdiction.[[74]](#footnote-74) The *Third Restatement of Foreign Relations Law* provides various factors for the courts to balance in making this determination. These factors include:

1. The link of the activity to the territory of the regulating state
2. The connection between the regulating state and the person principally responsible
3. The character of the activity
4. Expectations
5. The Importance of regulation to international political legal or economic systems
6. The extent to which the regulations consistent with international law
7. The extent to which another state may have an interest
8. The likelihood of conflict with regulation of another state

The concept of reasonableness described in the Third Restatement is also closely aligned with the legal doctrine of comity. Comity requires that states should generally avoid extraterritorial application of their laws against foreign citizens where those laws conflict. Where states have concurrent jurisdiction over an individual or a particular act, state should do a balancing test and defer to the state whose interests are clearly greater.[[75]](#footnote-75)

In Internet-related cases, determining whether a jurisdictional basis should be exercised can be quite complex. The courts may consider the place where the data controller is established, the place where the personal data is stored or processed, the place where the allegedly wrongful act occurs, the residents of the date subject, and the use of cookies or similar technologies in another state.[[76]](#footnote-76) Jurisdiction is based on the location of the data controller or the location where marketing email is received, the exercise of that jurisdiction tends to be accepted under the territoriality principle and effects doctrine.[[77]](#footnote-77) On the other hand, a more tenuous connection, such as the use of a single tracking cookie, might be viewed with greater skepticism.

Ultimately, the strongest grounds for a regulator to assert jurisdiction over a non-EU publisher would be to base it on a combination of the objective territoriality principle, the passive personality principle, and the effects test.[[78]](#footnote-78) It could be argued that such an assertion of jurisdiction would nonetheless be unreasonable under the Third Restatement test or otherwise violate the principles of comity. A successful argument against the application of the GDPR would likely require showing that it conflicted with a US law or regulation, such as the First Amendment free speech and free press protections, and that the publishers free expression interests outweigh the European Union’s interest in safeguarding its citizens privacy rights. Such an argument could also be supported by the fact that is often difficult or impossible for a publisher to know, with certainty, the geographic location of a user of its services.

**What to Expect from Courts**

Under the bases for international jurisdiction described above, it seems likely that European courts could find that the GDPR’s jurisdiction does extend to US publishers with websites that employ standard Internet advertising practices.[[79]](#footnote-79) It is not clear how courts would balance the right to privacy, which is considered a fundamental human right in Europe, against freedom of speech, a foundational right enshrined in the US Constitution. Certainly, it is conceivable that a European court would order a US-based publisher to comply. However, one possible argument a publisher could make against a right to be forgotten case, would be to argue that in order to alter the contents of the newspaper is not a proportional response to the petitioner’s privacy concern. Proportionality is a cornerstone in EU law and has been invoked in every right to be forgotten case. The publisher could also argue that the GDPR can only apply to the personal data of the EU citizens that gave rise to the GDPR’s jurisdiction in the first place. Article 3 of the GDPR says that the regulation “applies to the processing of personal data … where the processing activities are related to: … the monitoring of [EU data subject] behavior as far as their behavior takes place within the union.”[[80]](#footnote-80) Construed narrowly, this would indicate that the GDPR applies only to the processing of personal Data use to monitor EU data subjects—in other words, it only applies to the data gathered through the use of monitoring strategies. If this is the case, then any enforcement action under the GDPR could not extend to the contents of the published articles.

Even if a European court were to issue an order to a US publisher, it’s unlikely that a US court would enforce an order that violates the First Amendment. Any right to be forgotten order directed at a newspaper would almost certainly be argued to be in violation of the First Amendment. In general, freedom of press can only be restricted to “prevent graven immediate danger to interest which the state may lawfully protect.” Further, the First Amendment protects the publication of “lawfully obtained truthful information about a matter of public significance … absent a need … of the highest order.”

Even if the GDPR is applicable to certain conduct of US companies under international law, penalties for violating the law may not actually be enforceable. The ability under international law to exercise jurisdiction over an individual through its courts is, also, limited by whether it is “reasonable.”[[81]](#footnote-81) Section 421 of the *Third Restatement of Foreign Relations Law* also lays out the criteria for reasonableness in this area.[[82]](#footnote-82) A foreign companies permanent physical presence in the state would likely qualify as reasonable grounds to assert jurisdiction, but exercising jurisdiction over a company located entirely outside the EU whose the use of browser cookies to track individuals in the EU would likely be viewed with greater skepticism.[[83]](#footnote-83) A European regulator could attempt to assert jurisdiction based on the effects of that monitoring within the state, but the publisher has a plausible argument that the use of cookies does not have a “substantial, direct, and foreseeable” effect and that it would therefore be unreasonable to assert jurisdiction on the basis of cookies alone.

Under the doctrine of comity, US courts will generally grant extraterritorial effect to the valid judgments of foreign courts. However, a US court must be satisfied the foreign court properly has jurisdiction. It is likely a European right to be forgotten order under the GDPR would be unable to satisfy this requirement. Even if the US court finds that the foreign court did have jurisdiction, comity does not extend to orders that are found to be contrary to public policy. Among the policy issues that are considered grounds for refusal to enforce foreign orders are those that implicate constitutional rights.[[84]](#footnote-84) For example, when a foreign judgment is one that would violate the First Amendment, courts have found that it violates public policy and is thus unenforceable. On this basis, courts have consistently refused to enforce UK orders related to libel, because English libel law is considered to be antithetical to First Amendment doctrine.[[85]](#footnote-85) An order or fine under the GDPR related to the right to be forgotten would almost certainly violate the First Amendment, and a US Court would likely refuse to enforce such an order from an EU court.

There are additional statutory arguments that support the position that any penalty would be unenforceable under US law. The Securing the Protection of our Enduring an Established Constitutional Heritage (SPEECH) Act was enacted in 2010 to codify the common law presumption against enforceability of foreign libel judgments in US courts. Although the speech act has rarely been invoked since its passage, its legislative history offers some evidence that Congress intended to prevent US courts from enforcing foreign laws that violate the First Amendment.[[86]](#footnote-86) Nevertheless, serious questions remain about the applicablility of the GDPR and other foreign laws to conduct that happens beyond a states borders. This is likely to further complicate current efforts to address privacy today, as will be addressed in the next section.

**Privacy Today**

As discussed above, the Brussels Effect has been and continues to be a vehicle for the Europe Union to set the tone globally for regulating privacy and being able to export privacy laws that are more stringent than the United States’ and other nations’ laws. For example, after the EU adopted the DPD in 1995, over 30 countries adopted EU-type privacy laws. Although there may be “…very little the United States can do to stop the EU from regulating…” areas such as internet privacy, the US, States, US businesses, and individuals have not chosen to do nothing in response to the EU adopting the “stringent privacy law with an extraterritorial reach,” the GDPR.[[87]](#footnote-87)

**US Businesses**

US companies have responded in different ways to the GDPR. Some US companies have pulled out of the EU market or blocked their websites from EU consumers, rather than “risk falling foul” of the GDPR or believing that the potential risks outweigh the benefits of operating in the EU. For example, in 2018, Drawbridge, which creates profiles of consumers to track them across various devices, announced that it was closing advertising business in the EU because it was unclear how the digital ad industry would ensure consumer consent.[[88]](#footnote-88) When the GDPR became effective, Payver, a dash cam application that collects data on roads and signs by paying people to film streets as their driving, discontinued its EU service and tweeted “‘Sorry European Payver users… Talk to your lawmakers…’”[[89]](#footnote-89) Even though Steel Roots, a Boston-based cyber security and compliance business, did not market to EU consumers it began blocking EU visitors to its site out of concerns that it would become subject to the GDPR if they bought its products or services.[[90]](#footnote-90)

Some video game makers blocked EU users from accessing some of their older video games because it was not worth the investment to update the games to meet GDPR requirements. According to Uber Entertainment’s chief executive, Jeremy Ables, the company shut down its game, Super Monday Night Combat, because large parts of the game would have to be re-written to comply with the GDPR. Rather than pulling out of the EU or blocking users, other companies moved forward with efforts to comply with the GDPR. For example, in 2018, Microsoft had more than 1,600 engineers working on projects related to the GDPR.[[91]](#footnote-91)

Other companies have tried to become more transparent in response. In order to comply with the GDPR, Acxiom, a data broker that provides information on more than 700 million people culled from sources such as voter records and vehicle registrations, revised its US and European online portals so that consumers can see what information Acxiom has about them. According to Acxiom’s chief data ethics officer, Shelia Colclasure, the GPDR “‘will set the tone for data protection around the world for the next 10 years.’”[[92]](#footnote-92) Two years prior to the effective date of the GDPR, Pitney Bowes, which powers location analytics and ecommerce sites in 100 countries for companies like Zillow ran 20 privacy risk assessments to analyze how data was collected and broken out in Europe as compared to the US. By 2018, it had completed more than 90 assessments and had a specific group in its marketing department that focused on determining what data met the GDPR’s consent requirements.[[93]](#footnote-93)

Facebook and other social media companies have modified there terms of service in an effort to comply with the GDPR. In 2018, Facebook announced plans to add a privacy center feature where users could choose what advertisers can collect from them and double the number of its employees that focus on safety and security to 20,000 by the end of 2018.[[94]](#footnote-94) In a 2018 blog post, Facebook described some of its GDPR compliance methods, such as asking users to agree to updated terms of service and data policy and if they wanted Facebook to use data from its partners, and allowing facial recognition technology.[[95]](#footnote-95) In 2017, Google also revamped its privacy dashboard to be more user-friendly.[[96]](#footnote-96) It also created a website that details how all of its businesses, like AdWords, DoubleClick, and AdSense, collect information to target ads and personalize users’ experiences.[[97]](#footnote-97)

As discussed further below, because of the GDPR and California’s CDPA, some US companies, especially tech companies, have shifted from warding off federal legislation on privacy to “working with policy makers to help shape potential new federal privacy legislation.”[[98]](#footnote-98) For example, in a 2018 statement, Facebook stated that it was “‘working with policy makers to craft privacy legislation that protects consumers, ensures people are in control of their information and promotes responsible innovation.’”[[99]](#footnote-99) Christopher Padilla, an IBM vice present stated that the tech industry “‘is recognizing that doing nothing is not an option. Business is playing a more active role…That’s crucial because if we don’t do something in collaboration with government, none of us will like what’s done to us.’”[[100]](#footnote-100)

**Congressional Privacy Proposals**

Partially in response to the enactments of the GDPR and California’s CDPA, as well as data privacy scandals such as the disclosure of Facebook users’ information to Cambridge Analytica, several federal online data privacy bills were introduced in Congress in 2018 and 2019 and hearings were held by several committees, such as the FTC’s April 2019 hearings on Competition and Consumer Protection in the 21st Century. Some of the bills provide for comprehensive federal privacy bill, others provide a general set of duties, and others pre-empt state privacy laws while others do not. As an example of a proposal for a comprehensive federal privacy law, in November 2018, Senator Ron Wyden (D-Oregon) introduced the Consumer Data Protection Act (CDPA), which has been described as mirroring the GDPR and if passed it “would overhaul privacy protections on par with” the GDPR.[[101]](#footnote-101) Under the CDPA, companies that generate over $50 million in annual revenue and collect personal information on over one million consumers would be required to comply with a minimum set of privacy and cybersecurity policies established by the FTC. Like the GDPR, violators of the CDPA could be assessed civil penalties of up to $50,000 per violation and 4 percent of their total gross revenue.[[102]](#footnote-102)

Specifically, companies would be required to establish and implement cyber security and privacy policies, practices, and procedures to protect personal information used, stored, or shared from improper access, disclosure, exposure, or use.[[103]](#footnote-103) Companies would also be required to assess the impact their high-risk automated decision and information systems have on accuracy, fairness, bias, discrimination, privacy, and security.[[104]](#footnote-104) Further, companies with annual revenues exceeding $1 billion or data on more than 50 million consumers would be required to file annual reports with the FTC detailing whether or not the company complied with the CDPA and senior executives, like CEOs, who certify false statements in the reports could be fined up to $5 million and/or imprisoned up to 20 years.[[105]](#footnote-105)

Under the CDPA, a “Do Not Track” data sharing opt-out website would be created that would allow consumers to opt out of third-party companies tracking them on the web by sharing and selling their data, or targeting advertisements based on their personal data. However, companies would be able to charge consumers, who want to use their products and services, but not have their information monetized.[[106]](#footnote-106) Also, consumers would have the right to request, review, and challenge inaccuracies in their personal information collected and stored by companies,[[107]](#footnote-107) much like under the GDPR. However, the bill does not preempt other state privacy laws. It also authorizes the creation of a Bureau of Technology within the FTC and the appointment of additional personnel in the FTC’s Division of Privacy and Identity Protection of the Bureau of Consumer Protection and its Enforcement Division.[[108]](#footnote-108)

Instead of a comprehensive law like the GDPR, the Data Care Act (DCA), which was introduced in 2018 by Senator Brian Schatz (D-Hawaii) and 14 other Senators, requires online service providers to meet duties of care, loyalty, and confidentiality.[[109]](#footnote-109) Under the first duty, the duty of care, online providers would be required to reasonably secure individuals’ identifying data, such as their Social Security, passport and credit card numbers, user names and passwords, finger prints, and other unique biometric data, from unauthorized access and promptly notify them of a breach of their sensitive data.[[110]](#footnote-110) The second duty, the duty of loyalty would prohibit providers from using users’ identifying data in any way that would benefit the provider to the detriment of the users and would result in foreseeable and material physical or financial harm or would be unexpected and highly offensive to them.[[111]](#footnote-111) Finally, under the duty of confidentiality, providers would be prohibited from disclosing or selling users’ identifying data with any other person except as would be consistent with the duties of care and loyalty or the other person enters into a contract with the providers agreeing to comply with the DCA’s three duties.[[112]](#footnote-112) The FTC, state attorneys general, and state consumer protection officers would be authorized to enforce the DCA.[[113]](#footnote-113) About the bill, Senator Schatz stated that it would “…help make sure that when people give online companies their information, it won’t be exploited.”[[114]](#footnote-114) Online service providers that violate the DCA would be liable to for civil penalties equal to the amount calculated by multiplying the greater number of days they were in violation of the act or the number of users who were harmed by the violation, but not in excess of applicable penalties under the FTC Act.[[115]](#footnote-115) The DCA is not meant to modify, limit, or supersede the operation of any other federal or state privacy or security statutes and regulations.[[116]](#footnote-116)

The Social Media Privacy Protection and Consumer Rights Act (SMPP), which was re-introduced in 2019 by Senators Amy Klobuchar (D-Minn.) and John Kennedy (R-La.), would require online platform operators to inform users prior to creating an account or using the platform that unless they opt-out, their personal data produced during their online behavior will be collected and used by the operator and third parties.[[117]](#footnote-117) However, operators would be able to deny certain services or complete access to users if the users’ privacy elections creates inoperability in the platform.[[118]](#footnote-118) The SMPP defines personal data as individually identifiable information, including email addresses, telephone numbers, protected health information, the content of messages, and geolocation information.[[119]](#footnote-119) Under the SMPP, operators would have to disclose how they will use users’ personal data, their internal policies for using the data, and their employees and contractors access to the data.[[120]](#footnote-120) Also, operators would be required to offer users, free of charge and in an electronic and easily assessable format, copies of their personal data that the operator had processed and to notify users within 72 hours of becoming aware that users’ data had been transmitted in violation of the security platform.[[121]](#footnote-121) Further, the operators would have to provide users with the terms of service in a form that is easily accessible, of reasonable length, clearly distinguishable from other matters, and uses clear, concise, and well organized language.[[122]](#footnote-122) At least once every two years, the operators would be required to audit the privacy or security program of their online platform (SMPP § 3(d)).

Lastly, in 2019, Senator Marco Rubio (R-FL) introduced the American Data Dissemination (ADD), which would preempt states’ privacy laws and require the FTC to submit detailed recommendations and regulations for privacy requirements that Congress could impose on internet providers that would be substantially similar to the requirements applicable against agencies under the Privacy Act of 1974, that Congress would be able to impose on private corporations.[[123]](#footnote-123) If Congress did not enact a law based on the FTC’s recommendations, the FTC could put into effect its own privacy rules.[[124]](#footnote-124) This, like all of the federal proposals, would be a move towards comprehensive privacy regulations with an emphasis on business and their responsibility to consumers. Yet, serious questions remain about the desirability of a one-size-fits-all solution, even within the US.

**Conclusion**

Modern technology increasingly blurs the line between what is public and private. The dominance of cell phones and computers have significantly changed the ways in which we live our lives and share information about ourselves. Social media, and the numerous scandals involving the use of data obtained through social media for ulterior purposes, force us to consider the value of privacy and the implications of the decisions we make. With the passage of the GDPR and it’s attempts to establish extraterritorial jurisdiction, greater privacy regulations in the US seem necessary, and perhaps inevitable. However, the difficult tasks lie ahead.

The literature surrounding privacy makes clear the privacy is not easy to understand or define. It is beyond the reach of this paper to discuss the various ways it has been defined in different contexts. Suffice to say, privacy is a complex social practice that differs over time and space. Is it possible for comprehensive privacy laws, such as the GDPR, to recognize cultural diversity and disagreements about the nature of privacy and how it should be balanced against competing values? In this regard, privacy seems more local than global. Without the ability to account for differences, comprehensive privacy reforms are unlikely to be able to respond to the needs of individuals within the different social, political, and economic systems around the world.

In the US, freedom of speech and the emphasis on business interests are just two of the many ways in which privacy is approached much differently. This has made it difficult for multinational corporations to navigate. In the past, corporations could modify their behavior by relocating facilities and equipment to avoid enforcement of the strictest laws. Although questions remain, this is more difficult under the GDPR, which has forced some larger corporations to spend considerable amounts of money in an effort to comply. Nevertheless, significant penalties have already been imposed.

In January 2019, the French regulator, the National Data Protection Commission (CNIL), fined Google 50 million Euros ($56.8 million US) for violating “the essential principles of the GDPR: transparency, information and consent.”[[125]](#footnote-125) The CNIL stated that the information Google provided users was not easily accessible, clear, or comprehensive and users were not able to fully understand the extent of the processing operations carried out by Google. For example, the purposes of processing data and the categories of data processed for these purposes were “described in a too generic and vague manner.”[[126]](#footnote-126) Also, the CNIL stated that Google users’ consent to process data for ads personalization purposes was not validly obtained as they were not sufficiently informed and their consent was neither specific nor unambiguous.

The stakes are high for corporations and individuals alike. Companies will be required to figure out how to comply with strict data privacy laws, or face significant fines, as legislatures struggle to balance privacy against other competing values. Individual privacy will continue to be sacrificed as US policymakers seek to protect corporations from unnecessary restrictions that might impact their ability to make profits and access markets. In the end, the United States is a capitalist economic system that relies on a vibrant network of private corporations that have a considerable influence on the creation of laws, as well as their enforcement. It is unlikely that meaningful privacy reforms will succeed until Americans, and they’re lawmakers recognize the fundamental nature of the right to privacy for human flourishing.

**Works Cited**

Bennett, Colin J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States 164-80.

Benn, S.I. (1971). Pennock, J.R. and Chapman J.W. editors. (1971). Privacy, freedom, and respect for persons, in privacy 1, 3-4.

Bignami, F. (2007). European versus American liberty: a comparative privacy analysis of antiterrorism data mining. Boston College Law Review. vol. 48. 609-698. (2007a).

Bignami, F. (2007). Privacy and law enforcement in the European Union: The data retention directive. Chicago Journal of International Law. vol. 8, 233-255. (2007b).

Bignami, F. (2008). The case for tolerant constitutional patriotism: the right to privacy before the European courts. Cornell International Law Journal. vol. 41, 211.

Bradford, A. (2012). The Brussels effect. Northwestern University Law Review. Vol 107, p. 1.

Brandeis, L. D., & Warren, S. D. (1890, December 15). The Right to Privacy. Harvard Law Review. IV(5).

Burri, M. and Schar, R. (2016). The reform of the EU Data Protection framework. Journal of Information Policy. vol. 6, 479.

Calder, A. (2016). EU GDPR: a pocket guide. IT Governance Publishing.

Cate, F.H. (1999). Changing face of privacy protection in the European Union and the United States. 33 Indiana Law Review 173.

Cunningham, M. (2016). Free expression, privacy, and diminishing sovereignty in the information age: the internationalization of censorship. Arkansas Law Review. vol. 69:71.

Davis, J. (2018, November 2). Proposed privacy bill mirrors GDPR, adds jail time for lying CEOs. Healthcare IT News.

Drozdiak, N. (2018, May 19). Data-privacy law creates new business for tech consultants. *Wall Street Journal.*

European Commission. Factsheet on the “right to be forgotten” ruling. c-131/12.

European Community. Foreign ministers of the six European Community countries. (1970, October 27). First report of the foreign ministers to the heads of state and government of the member states of the European Community. Part One P 5.

Federal Trade Commission. (1998, August 13). Internet site agrees to settle FTC charges of deceptively collecting personal information in Agency’s first internet privacy case. Press Release.

FTC File No. 982 3015. <https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting>.

Federal Trade Commission. (2019). Privacy and security enforcement. <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement>.

Federal Trade Commission. (2019, March 15). FTC releases 2018 privacy and data security update. <https://www.ftc.gov/news-events/press-releases/2019/03/ftc-releases-2018-privacy-data-security-update>.

Green. D. The SPEEC Act provides protection against foreign libel judgments. American Bar Association. http://apps.americanbar.org.mimas.calstatela.edu/litigation/litigationnews/mobile/firstamendment-SPEECH.html (last visited Feb. 24, 2018)

Hadjipetrova, Ganka, Poteat, Hannah G. (2014, July and August). States are coming to the fore of privacy in the digital era. Landslide. Vol. 6, Issue 6.

Johnson, L. (2018, February 26). GDPR: What companies need to know. Adweek.

Karaduman, O. (2017, September). The General Data Protection Regulation: achieving compliance for EU and non-EU companies. Business Law International. vol. 18, No. 3. 225.

Kelso, J.C. (1992, January 15). California’s constitutional right to privacy. Pepperdine Law Review. vol. 19 issue 2 article 1.

Kennedy, J. (2019, January 18). Sens. Kennedy, Klobuchar Introduce Bipartisan Legislation To Protect Privacy of Consumers’ Online Data. https://www.kennedy.senate.gov/public/2019/1/sens-kennedy-klobuchar-introduce-bipartisan-legislation-to-protect-privacy-of-consumers-online-data.

Kenyon, A.T. and Richardson, M. editors. (2006). New dimensions in privacy law: international and comparative perspectives. Cambridge: Cambridge University Press.

Kuchler, H. (2018, May 24). US companies wrestle with new European privacy rules*. Financial Times.*

Kumm, M. (2008) Why Europeans will not embrace constitutional patriotism. International Journal of Constitutional Law. vol. 6, 117, 120.

Kuner, C. (2010). Data protection law and international jurisdiction on the internet (part I). Internationl Journal of Law and Informational Technology. Vol 176, 179-180.

Lazarus, D. (2012, February 24). Privacy, online is so passe. *Los Angeles Times*.

Liebelson, D. (2013, March 1). First SOPA, now your privacy: Facebook, Google flex lobbying muscle in Europe. *Mother Jones*. Accessed on March 20, 2013 at

”http://www.motherjones.com/politics/2013/03/google-facebook-sopa-privacy.

Magic, P. (2018, June 27). How small businesses can survive in the age of GDPR. https://www.entrepreneur.com/article/315366

Margalit, A. (1971). Goldblum, N. translator. (1996). The decent society. 202-04.

Mckinnon, J.D. and Vartabedian, M. (2018, August 6). Tech firms, embattled over privacy, warm to federal regulations. *Wall Street Journal*.

National Data Protection Commission. (2019, January 21). The CNIL’s restricted committee imposes financial penalty of 50 million euros against GOOGLE LLC. <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.

O'Brien, D. (1902). The right of privacy. Columbia Law Review, 2, 437.

O’Brien, K.J. (2013, January 25). Silicon Valley companies lobbying against Europe’s privacy proposals. *New York Times*.

Organisation for Economic Co-operation and Development. (1980, October 1, as amended on 2013, July 11). Guidelines on Protection of Privacy and Transborder Flows of Personal Data. Document c58 final.

Organisation for Economic Co-operation and Development. (2011). Thirty years after the OECD Privacy Guidelines.

Ovey, C. and White, R. (4th ed. 2006*).* Jacobs and White: The European Convention on Human Rights. 3.

Parker, S. (2018, December 5). A step forward for federal privacy legislation. Harvard Journal of Law & Technology.

Prosser, W. L. (1960, August). Privacy. California Law Review. 48(3), 383-423.

Reding, V. (2010, June 22). Fundamental rights and citizenship. Speech to American Chamber of Commerce to the EU. SPEECH-10-327.

Reding, V. (2013, March 26). EU data protection rules: better for business, better for citizens. Speech to European Parliament.

Ryngaert, C. (2015). Symposium issue on extraterritoriality and EU data protection, 5 Internation Data Privacy Law 221.

Rubio, M. (2019, January 16). Rubio introduces privacy bill to protect customers while promoting innovation. <https://www.rubio.senate.gov/public/index.cfm/2019/1/rubio-introduces-privacy-bill-to-protect-consumers-while-promoting-innovation>.

Schatz, B. (2018, December 12). Schatz leads group of 15 senators in introducing new bill to help protect people’s personal data online. <https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online>.

Schwartz, P.M. and Solove, D.J. (2014, August). Reconciling personal information in the United States and European Union. California Law Review. Volume 102:877.

Second Restatement of Torts. §§ 652A-652I (1977).

Shepard, G. (2018, April 25). GDPR and what it means for your business. Forbes Technology Council.

Social Media Privacy Protection and Consumer Rights Act, SIL 18B29, 116th Cong. 1st Session (2019).

Tashea, J. (2018, March). A new era: companies and their lawyers are bracing for a wide-ranging EU data-privacy law that takes effect in May. American Bar Association. vol. 104. issue 3, 8.

Thompson II, R.M. and Cole, J.P. (2015, May 19). Stored Communications Act: reform of the Electronic Communications Privacy Act (ECPA). Congressional Research Service.

Tiku, N. (2018, March 19). Europe’s new privacy law will change the web and more. Wired.

Timberg, C. (2013, March 14). Web browsers consider limiting how much they track users. *The Washington Post*.

United States Department of Health, Education and Welfare Secretary’s Advisory Committee on Automated Personnel Data Systems. (1973, July). Records, Computers and the Rights of Citizens.

United States Government Accountability Office. (2019, January). Internet privacy additional federal authority could enhance consumer protection and provide flexibility. GAO-19-52.

Ustaran, E. , Room, S., Rudgard, S., Hordern, V., Lee, P., Pastor, N., Patrikios, A., Jackson, H., Levin, M., and Taranto, L. (2012). Chapter 1: Origins and historical context of data protection law.

Vogel, D. (1997). Trading up and governing across: transational governance and environmental protection. Jounral Europe Public Policy. Vol 4, p. 556.

European privacy: law and practice for data protection professionals. International Association of Privacy Professionals.

Voss, W.G. (2012, November). Preparing for the proposed EU General Data Regulation: with or without amendments. American Bar Association. Business Law Today.

Warren, S. and Brandeis, L., (1890), “The Right to Privacy,” *Harvard Law Review*, Vol. 4, pp. 193–220.

Watanabe, P.J. (2017). An ocean apart: the transatlantic data privacy divide and the right to erasure. Southern California Law Review. Volume 90: 1111.

Westin, Alan (1967) Privacy and Freedom, IG Publishing: New York.

Whitman, J.Q. (2004). The two western cultures of privacy: dignity versus liberty. 113 Yale Law Review 1151, 1173-76.

Wimmer, Kurt (2018) “Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers,” Syracuse Law Review, Vol. 68, pp. 547-578.

Wyden, R. (2018, November 1). Wyden releases discussion draft of legislation to provide real protections for Americans’ Privacy. https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.

**Cases**

*Abdullah vs. Sheridan Square Press, Inc*., No. 93-CV-2515, 1994 WL 419847, at \*1 (S.D.N.Y. May 4, 1994)) (mem.).

*Bachchan vs. India Abroad Publ'ns, Inc*., 585 N.Y.S.2d 661, 664 (N.Y. Sup. Ct. 1992).

*de la Mata vs. Am. Life Ins. Co.*, 771 F. Supp. 1375, 1384 (D. Del. 1991).

*Griswold v Connecticut*, 381 U.S. 479 (1965).

*Hartford Fire Ins. Co. vs. California*, 509 U.S. 764, 796 (1993).

*Koster v. Automark Indus.*, 640 F.2d 77, 79 (7th Cir. 1981).

*Matsushita Elec. Indus. Co. vs. Zenith Radio Corp*., 475 U.S. 574, 582 (1986).

*Olmstead v. United States*, 277 U.S. 438 (1928).

**Statutes**

15 United States Code §§ 6801 and 6802.

18 United States Code §§ 2510, 2518, 2702, 2703, 2710, and 2711.

26 United States Code §§ 6103.

American Data Dissemination Act of 2019, OLL19040, 116th Cong. 1st Session (2019).

California Constitution. Art. I, § 1 (amended 1972).

California Civil Code §§ 1798.83, 1798.84, 1798.100 and 1798.105.

California Public Utilities Code §§ 2891 to 2894.10.

Charter of Fundamental Rights of the European Union, Dec. 7, 2000, 2000 O.J. (C 364) 1, 7-8.

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 5(b), Jan. 28, 1981, Eur. T.S. No. 108, art. 3.

Council of Europe Resolution 73/22.

Council of Europe Resolution 74/29.

Children’s Online Privacy Protection Act of 1998, Public Law Number 105-277, 112 Statute 2681-728.

Communications Act of 1934, Public Law Number, 73-416, 48 Statute 1064.

Consumer Data Protection Act, SIL 18B29, 115th Cong. 2d Session (2018).

Data Care Act, SIL 18B29, 115th Cong. 2d Session (2018).

Electronic Communications Privacy Act of 1986, Public Law Number 99-508, 100 Statute 1848.

European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

European Union Data Protection Directive. Directive 95/46/E.C., 1995 O.J. (L 281) 31-32.

Financial Services Modernization Act of 1999, Public Law Number 106-102, 113 Statute 1338.

Gramm-Leach-Bliley Act of 1999, Public Law Number 106-112, 113 Statute 1338.

Fair and Accurate Credit Transactions Act of 2003, Public Law Number 108-159, 117 Statute 1952.

Federal Trade Commission Act of 1914, Public Law Number 111-2, 38 Statute 717.

Health Insurance Portability and Accountability Act of 1996, Public Law Number 104-191, 110 Statute 1936.

Omnibus Crime and Control Act of 1968, Public Law Number 90-351, 82 Statute 197.

Privacy Act of 1974, Public Law Number 93-579, 88 Statute 1896.

Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act of 2010, Public Law Number 111-223, 124 Statute 2480-2484.

United Nations General Assembly. (1948). Universal Declaration of Human Rights (217 [III] A). Paris.

Video Privacy Protection Act of 1988, Public Law Number 100-618, 102 Statute 3195.

Video Privacy Protection Act Amendments Act of 2012, Public Law Number 112-258, 126 Statute 2414.

1. 2016/679. [↑](#footnote-ref-1)
2. *See* Westin (1967). [↑](#footnote-ref-2)
3. Schwartz and Solove 2014, 880-881; Whitman 2004; Cunningham 2016; Watanabe 2017. [↑](#footnote-ref-3)
4. ECHR Art.10. [↑](#footnote-ref-4)
5. EU Directive 95/46/EC. [↑](#footnote-ref-5)
6. DPD Art. 1. [↑](#footnote-ref-6)
7. Schwartz and Solove 2014; Watanabe 2017. [↑](#footnote-ref-7)
8. DPD Art. 2(d) defines a controller as a “…. natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.” [↑](#footnote-ref-8)
9. DPD Art. 4(1). [↑](#footnote-ref-9)
10. DPD Art. 25(1). [↑](#footnote-ref-10)
11. DPD Art. 25(6) [↑](#footnote-ref-11)
12. GDPR Arts. 94 and 99; European Commission 2018; Watanabe 2017. In the EU, a directive, such as the DPD, defines the results to be achieved by the directive and leaves the choice of how to achieve the results up to the EU’s member states. Whereas, a regulation, such as the GDPR, is directly applicable to the member states, has the legal effect independent of the member states’ laws, and overrides their laws that are contrary to the regulation (Schwartz and Solove 2014). [↑](#footnote-ref-12)
13. Burri 2016; Drozdiak 2018. [↑](#footnote-ref-13)
14. GDPR Art. 2. The GDPR defines personal data as “…any information relating to an identified or identifiable natural person…” (GDPR Art. 4(1)). An identifiable natural person is someone who can be directly or indirectly identified by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person (GDPR Art. 4(1)). [↑](#footnote-ref-14)
15. European Commission 2018. [↑](#footnote-ref-15)
16. GDPR Arts. 3(1), 4(7) and 4(8). [↑](#footnote-ref-16)
17. GDPR Art. 3(2). [↑](#footnote-ref-17)
18. GDPR Art. 2(2). [↑](#footnote-ref-18)
19. GDPR Arts. 6(1)(a) and 7. Processing is defined as “… any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” (GDPR Art. 4(2)). [↑](#footnote-ref-19)
20. GDPR Art. 6. Consent of an individual “…means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (GDPR Art. 4(11)). If a child is younger than 16 years old, the processing of their personal data is lawful only if and to the extent the child’s holder of parental responsibility gives or authorizes consent (GDPR Art. 8). [↑](#footnote-ref-20)
21. GDPR Art. 16. [↑](#footnote-ref-21)
22. GDPR Art. 17(1). [↑](#footnote-ref-22)
23. GDPR Art. 17(3). [↑](#footnote-ref-23)
24. GDPR Art. 83(5). [↑](#footnote-ref-24)
25. Brandeis & Warren, 1890. The *Harvard Law Review* article titled “The Right to Privacy,” was written after the *Saturday Evening Gazette* published embarrassing details of Samuel D. Warren’s daughter’s wedding. Mr. Warren, who had recently given up the practice of law to devote himself to an inherited business, became annoyed and turned to his recent law partner, Louis D. Brandeis. The two collaborated on the article, although it has been suggested that Brandeis most likely did most of the work (Prosser, 1960). In the article, Brandeis and Warren announced confidently that “the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.” Brandeis eventually became a U.S. Supreme Court Justice and was given the opportunity to further articulate, what he referred to as “the right to be let alone.” In his dissent in *Olmstead v. United States* (1928), he echoed the importance of privacy he had argued for in his law review article many years earlier, calling it, “the most comprehensive of rights and the right most valued by civilized men” (*Olmstead v. United States*, 1928). Justice Brandeis went on to suggest that, “[to protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment” (*Olmstead v. United States*, 1928 (Brandeis,J., dissenting)). [↑](#footnote-ref-25)
26. Prosser 1960. [↑](#footnote-ref-26)
27. *Id.* [↑](#footnote-ref-27)
28. *Id.* [↑](#footnote-ref-28)
29. *Id.* [↑](#footnote-ref-29)
30. *Id.* [↑](#footnote-ref-30)
31. *Griswold vs. Connecticut 1965*; Cate 1999; Whitman 2004; Cunningham 2016. [↑](#footnote-ref-31)
32. The case involved a Connecticut law that made it a crime to use any “drug, medicinal article or instrument for the purpose of preventing conception” (*Griswold v. Connecticut*, 1965). Estelle Griswold was the Executive Director of the Planned Parenthood League of Connecticut. Dr. C. Lee Buxton was a licensed physician and a professor at the Yale Medical School and served as the Medical Director for the League at its center in New Haven. The center was open for about 10 days in November of 1961 when Griswold and Buxton were arrested and convicted for giving “information, instruction, and medical advice to married persons as to the means of preventing conception” (*Griswold v, Connecticut*, 1965). The USSC overturned Griswold’s and Buxton’s convictions. [↑](#footnote-ref-32)
33. *Griswold vs. Connecticut* 1965. [↑](#footnote-ref-33)
34. Cate 1999; Schwartz and Solove 2014; Cunningham 2016; GAO, 2019, 6. [↑](#footnote-ref-34)
35. Morrison 2008. [↑](#footnote-ref-35)
36. 18 U.S. Code § 2702(a)(1). [↑](#footnote-ref-36)
37. 18 U.S. Code §§ 2510, 2702(a)(2) and 2711. [↑](#footnote-ref-37)
38. 18 U.S. Code §§ 2702(a)(3) and (c). [↑](#footnote-ref-38)
39. 18 U.S. Code §§ 2703(a) and (d). [↑](#footnote-ref-39)
40. 15 U.S. Code § 6801(a). [↑](#footnote-ref-40)
41. 15 U.S. Code §§ 6802(a) and (b). [↑](#footnote-ref-41)
42. 15 U.S. Code § 6802(b). [↑](#footnote-ref-42)
43. FTC March 2019. [↑](#footnote-ref-43)
44. 15 U.S. Code §§ 41-58; FTC 2019. [↑](#footnote-ref-44)
45. FTC 1998. [↑](#footnote-ref-45)
46. GAO 2019. [↑](#footnote-ref-46)
47. Cate 1999. [↑](#footnote-ref-47)
48. Hadjipetrova 2014. [↑](#footnote-ref-48)
49. California Civil Code §§ 22575- 22578. [↑](#footnote-ref-49)
50. California Civil Code §§ 1798.100; 1798.105; 1798.120; 1798.140(g); and 1798.140(o). [↑](#footnote-ref-50)
51. California Civil Code § 1798.120. [↑](#footnote-ref-51)
52. California Civil Code § 1798.140(c). [↑](#footnote-ref-52)
53. California Civil Code § 1798.155. [↑](#footnote-ref-53)
54. Vogel 1997; Bradford 2012; Hadjipetrova 2014. [↑](#footnote-ref-54)
55. Bradford 2012, 5; Hadijpetrova 2014. [↑](#footnote-ref-55)
56. Hadjipetrova 2014. [↑](#footnote-ref-56)
57. Bradford 2012, 50. [↑](#footnote-ref-57)
58. *Id.* at 3 and 5. [↑](#footnote-ref-58)
59. Bradford 2012, 4. [↑](#footnote-ref-59)
60. *Id.* at 3. [↑](#footnote-ref-60)
61. Wimmer 2018. [↑](#footnote-ref-61)
62. *See* Wimmer 2018, 557; and Rochester 80. [↑](#footnote-ref-62)
63. Wimmer 2018 (citing Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part I)*, 18 INT'L J. L. & INFO. TECH. 176, at 188 and 190). [↑](#footnote-ref-63)
64. Restatement (Third) of Foreign Relations Law § 402(1)(a)--(b). [↑](#footnote-ref-64)
65. Kuner 2010, *supra* note 64 at 188. [↑](#footnote-ref-65)
66. Council Directive 95/46/EC, art. 4, 1995 O.J. (L 281). [↑](#footnote-ref-66)
67. *See* Restatement (Third) of Foreign Relations Law § 402. [↑](#footnote-ref-67)
68. *Id.* [↑](#footnote-ref-68)
69. Kuner 2010, *supra* note 64 at 188. [↑](#footnote-ref-69)
70. Restatement (Third) of Foreign Relations Law § 402(3). [↑](#footnote-ref-70)
71. Id. § 402(1)(c); Kuner, supra note 64, at 190; see *Hartford Fire Ins. Co. vs. California*, 509 U.S. 764, 796 (1993) (citing *Matsushita Elec. Indus. Co. vs. Zenith Radio Corp*., 475 U.S. 574, 582 (1986)) (“[A domestic law] applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States.”). [↑](#footnote-ref-71)
72. Kuner 2010, supra note 64, at 190. [↑](#footnote-ref-72)
73. *Id.* [↑](#footnote-ref-73)
74. Restatement (Third) of Foreign Relations Law § 403(1). [↑](#footnote-ref-74)
75. *Id.* [↑](#footnote-ref-75)
76. Kuner 2010, *supra* note 64, at 237-40. [↑](#footnote-ref-76)
77. *Id.* at 241. [↑](#footnote-ref-77)
78. Ryngaert 2015, 222. [↑](#footnote-ref-78)
79. Wimmer 2018, 561 and 562. [↑](#footnote-ref-79)
80. Council Regulation 2016/679, *supra* note 2, at 32-33. [↑](#footnote-ref-80)
81. Restatement (Third) of Foreign Relations Law, pt. IV, ch. 3, intro. note (AM. LAW INST. 1987). § 421 cmt. a. [↑](#footnote-ref-81)
82. Restatement (Third) of Foreign Relations Law § 421. [↑](#footnote-ref-82)
83. Kuner 2010, *supra* note 64, at 235. [↑](#footnote-ref-83)
84. *See, e.g*., *de la Mata vs. Am. Life Ins. Co.*, 771 F. Supp. 1375, 1384 (D. Del. 1991) (citing *Koster v. Automark Indus.*, 640 F.2d 77, 79 (7th Cir. 1981)) (discussing the consideration of due process). [↑](#footnote-ref-84)
85. *See Id*. at 3-4 (citing *Abdullah vs. Sheridan Square Press, Inc*., No. 93-CV-2515, 1994 WL 419847, at \*1 (S.D.N.Y. May 4, 1994)) (mem.) (“Since establishment of a claim under the British law of defamation would be antithetical to the First Amendment protections accorded the defendants, the second cause of action alleged in the complaint is dismissed.”); *Bachchan vs. India Abroad Publ'ns, Inc*., 585 N.Y.S.2d 661, 664 (N.Y. Sup. Ct. 1992) (“[Denying summary judgment because] [t]he protection to free speech and the press embodied in [the First Amendment] would be seriously jeopardized by the entry of foreign libel judgments granted pursuant to standards deemed appropriate in England but considered antithetical to the protections afforded the press by the US Constitution.”). [↑](#footnote-ref-85)
86. Dana Green, The SPEECH Act Provides Protection Against Foreign Libel Judgments, AM. BAR ASS'N, http://apps.americanbar.org.mimas.calstatela.edu/litigation/litigationnews/mobile/firstamendment-SPEECH.html (last visited Feb. 24, 2018) (“The act's symbolic significance, as an expression of the depth of Congressional commitment to free speech, should be heartening to free speech advocates.”). [↑](#footnote-ref-86)
87. Bradford 2012, 50. [↑](#footnote-ref-87)
88. Tiku 2018. [↑](#footnote-ref-88)
89. Kuchler 2018. [↑](#footnote-ref-89)
90. . *Id.* [↑](#footnote-ref-90)
91. *Id.* [↑](#footnote-ref-91)
92. Tiku 2018. [↑](#footnote-ref-92)
93. Lauren 2018. [↑](#footnote-ref-93)
94. Johnson 2018. [↑](#footnote-ref-94)
95. Magic 2018. [↑](#footnote-ref-95)
96. Tiku 2018. [↑](#footnote-ref-96)
97. Johnson 2018. [↑](#footnote-ref-97)
98. McKinnon 2018. [↑](#footnote-ref-98)
99. McKinnon 2018. [↑](#footnote-ref-99)
100. McKinnon 2018. [↑](#footnote-ref-100)
101. Davis 2018. [↑](#footnote-ref-101)
102. CDPA §§ 2(5) and 4. [↑](#footnote-ref-102)
103. CDPA § 7(b). [↑](#footnote-ref-103)
104. CDPA § 7. [↑](#footnote-ref-104)
105. CDPA § 5(a). [↑](#footnote-ref-105)
106. CDPA § 6(a). [↑](#footnote-ref-106)
107. CDPA § 7. [↑](#footnote-ref-107)
108. CDPA §§ 8 and 9. [↑](#footnote-ref-108)
109. DCA § 3(a). [↑](#footnote-ref-109)
110. DCA §§ 2(5) and 3(b)(1). [↑](#footnote-ref-110)
111. DCA § 3(b)(2). [↑](#footnote-ref-111)
112. DCA § 3(b)(3). [↑](#footnote-ref-112)
113. DCA §§ 4(a) and (b). [↑](#footnote-ref-113)
114. Schatz 2018. [↑](#footnote-ref-114)
115. DCA § 4(b)(2). [↑](#footnote-ref-115)
116. DCA § 6. [↑](#footnote-ref-116)
117. SMPP § 3(a)(1)(A). [↑](#footnote-ref-117)
118. SMPP § 3(a)(1)(B). [↑](#footnote-ref-118)
119. SMPP § 2(6). [↑](#footnote-ref-119)
120. SMPP § 3(a)(1)(D). [↑](#footnote-ref-120)
121. SMPP §§ 3(b) and 3(c). [↑](#footnote-ref-121)
122. SMPP § 3(a)(1)(C). [↑](#footnote-ref-122)
123. ADD §§ 2(5), 3(a), 4(a)(1), and 6. [↑](#footnote-ref-123)
124. ADD § 4(a)(2). [↑](#footnote-ref-124)
125. CNIL 2019. [↑](#footnote-ref-125)
126. CNIL 2019. [↑](#footnote-ref-126)