Ethics of Smart Meters and Connected and Autonomous Vehicles:

Privacy Regulations in the U.S. and the European Union

By Magdalena N. Sudibjo, Sociology Department, Vanderbilt University

Under review, Science and Engineering Ethics.

Not for circulation outside the spring 2019 PIRE seminar.

**Abstract**

The advent of the internet of things has brought with it new challenges for privacy protection. Especially as privacy breaches continue to become more frequent, the development of privacy protection for these new technologies becomes more urgent. This paper focuses on the privacy implications and regulations of two, emerging connected technologies: smart meters and connected and autonomous vehicles (CAVs). More specifically, this paper adds to prior discussions on the ethics behind technology by providing a comparative review of the privacy protection concerning these two technologies in the U.S. and the European Union. A comparative approach can help identify gaps as well as possible solutions and future directions. Different approaches to privacy protection also suggests differences in underlying ethical frameworks. The ethical principles behind privacy regulation should be considered when developing future privacy protection.

**Introduction**

 The privacy implications of technology have become a topic of growing importance in recent years, especially as a barrage of privacy breaches due to technology has come to light. For example, the 2018 fallout from the Cambridge Analytica scandal exposed the unapproved use of over 50 million Facebook users’ personal information that was appropriated in an attempt to influence the 2016 U.S. presidential election (Granville 2018). As these increasingly frequent incidences illustrate, technological advancement has allowed the gathering and storing of enormous amounts of personal data, yet data protection and privacy regulation have struggled to keep pace. More work is needed not only in creating regulation but also in outlining the ethical principles that guide both policy and design decisions.

This study provides a comparative review of the privacy principles and regulations related to two new and emerging technologies: smart meters and connected and autonomous vehicles (CAVs). Both technologies have become a growing part of people’s daily lives, and each technology provides different challenges for those concerned with privacy and data protection. Prior research has considered specific questions concerning these technologies, such as who is liable for CAV accidents (e.g. Hevelke and Nida-Rümelin 2015) or what ethical guidelines should be embodied in these technologies (e.g. Gogoll and Müller 2017). Other studies consider how a broad range of values, such as social justice, safety, and sustainability, can be integrated into the design of technology (e.g. Flipse and Puylaert 2018, Mladenovic and McPherson 2016). However, to date there has been no systematic comparison of the privacy dimensions of these two technologies in the European Union (E.U.) and the U.S. A broad comparative overview of the progress in privacy protection for these technologies can help to identify successes, gaps, and possible future directions for governmental bodies and system engineers. A comparison between the U.S. and the E.U. also reveals how differences in underlying ethical frameworks are associated with differences in regulatory policy. A consideration of the principles behind regulations can help improve future privacy protections.

This paper is structured into five sections. The first section describes the risks to privacy of smart meters and CAVs. The second section discusses three different approaches to privacy protection, including both regulatory and design approaches. The next two sections provide an overview of the current data protections—both in general terms and with respect to smart meter and CAV technologies— that are in place in the U.S. and the E.U. respectively. Finally, this paper ends with a discussion of what can be learned from the comparison between the U.S. and E.U. as well as a discussion of gaps and policy suggestions.

**Risks to Privacy: Smart Meters and CAVs**

Both smart meters and CAVs offer substantial potential benefits to the utilities and customers. Smart meters enable the energy-service company to gather energy usage data at very short intervals and to communicate bi-directionally with utility companies. The remote communication possibility is in contrast with analog meters, which require an employee to gather this information by visiting the building. This remote-communication capacity allows the utilities to engage in advanced demand management and to identify power outages more precisely and quickly. Moreover, energy consumers may gain economic benefits from adapting to real-time information about their energy usage, which may in turn lead to improvements in environmental sustainability (Stephens, Wilson, and Peterson 2015). Connected vehicles also enable remote communication, both among vehicles and with remote agents, and an autonomous vehicle is a type of connected vehicle that contains advanced driver assistance technology and the potential for operation without a driver. CAVs can offer several potential benefits, including lessening traffic congestion, lowering traffic accidents caused by human error, improving access to transportation for those unable to drive, and increasing highway capacity (Bagloee et al. 2016, Ramos 2016). Besides these direct benefits, improved traffic may also lead to a reduction in public costs associated with accident prevention, healthcare, as well as greenhouse gas emissions (Bonneau et al. 2017).

Although the potential benefits of these technologies are substantial, both smart meters and CAVs pose various types of risks, including those associated with privacy and security. Because smart meters are able to gather and store very detailed information about a household’s energy usage, hackers may be able to access the data and use the information to track when people are not at home or for other nefarious purposes (McDaniel and McLaughlin 2009). Likewise, CAVs gather information about the driver’s travel locations and timing, and consumer groups worry that hackers will be able to access a car’s system and take control of the vehicle. Studies have found that security intelligence experts were able to hack into a CAV and take control of its driving functions (Greenberg 2015). Moreover, CAVs equipped with cameras, radar, and LIDAR can gather not only the driver’s personal data but also data from the environment, such as other vehicles’ license plates or pedestrians’ faces, which are all considered personal data (Taeger 2017).

These risks are important to address not only for security and safety reasons but also for gaining public acceptance of these technologies. A survey released by Consumer Watchdog found that 79 percent of respondents were concerned about the security of the data collected by CAVs, while 75 percent said that Congress “should apply the brakes on driverless cars until technology is proven safe” (Public Policy Polling 2018). Similarly, the American Automobile Association found that 73 percent of U.S. drivers in 2018, compared to 63 percent in 2017, stated that they “would be afraid to ride in a fully-self-driving vehicle” (Edmonds 2018). These results were published following a series of CAV-related accidents, some of which resulted in fatalities, in 2017 and 2018. Similarly, Hess (2014) finds that privacy and security concerns are one of the main reasons for organized public opposition to smart meters. Several civil society organizations have been vocal and active over these issues. For example, the Center for Electrosmog Prevention and the Utility Reform Network cite privacy concerns in their campaign for an opt-out option for smart meters, which are often installed without home owners’ knowledge or permission (California Public Utilities Commission 2011). In sum, both smart meters and CAVs provide new challenges to privacy that need to be addressed.

**Approaches to Privacy for Advanced Technologies**

The Fair Information Practice Principles (FIPPs) and the Principles of Privacy by Design constitute two starting points for developing guidelines for privacy regulation and software development. This section will also review a third framework for approaching privacy protection called contextual integrity, which offers a more flexible approach than the previous two.

*Fair Information Practice Principles*

The idea for FIPPs originated in the late 1960s and early 1970s, when computers began to increase their capability for information processing, and the public became concerned with the risks to privacy that these new technologies presented (Bennet 2008). In response, policymakers developed a set of basic guidelines for the protection of privacy and the security of data. Although different organizations have since enumerated these principles in slightly different ways, the content of these guidelines are essentially the same. The Privacy Office of the U.S. Department of Homeland Security summarizes the FIPPs principles as follows (Dahn 2014):

1. *Transparency*: Organizations should provide notice to individuals about their policies and practices.
2. *Individual participation*: Individuals must give their consent prior to data collection and processing.
3. *Purpose specification:* Organizations should specifically articulate the purposes for which the information is to be used at or prior to the time of data collection.
4. *Data minimization*: Organizations should only collect the minimal amount of data necessary to complete the stated purpose.
5. *Use limitation*: Data should only be used for the purposes that has been identified.
6. *Data quality and integrity*: Organizations should make sure that data is accurate, relevant, and complete and should allow individuals to contest and correct their data
7. *Data security*: Organizations should ensure that the collected data are protected against risks such as loss, unauthorized access, destruction, or unintended modification.
8. *Accountability and Auditing*: Organizations should be accountable for complying with these principle and demonstrate their compliance.

Although governments and organizations may disagree about the best method for complying with or enforcing these principles, FIPPs have become widely adopted, either explicitly or implicitly, by many national governments around the world, including in the U.S., Canada, New Zealand, and Australia, as well as by a number of international organizations, such as the Organization for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), and the Council of Europe. Article 5 of the E.U.’s General Data Protection Regulation (GDPR) outlines similar principles and issues a monetary fine for noncompliance (European Commission 2016).

*Privacy by Design*

While policy experts work on safeguarding privacy by regulating organizations and technologies, system engineers have developed an approach called privacy by design, which refers to the proactive embedding of privacy in all aspects of a system’s development. Thus, rather than regulating privacy “downstream,” or after a technology has been developed, these engineers work on “upstream” safeguards that prevent privacy breaches by building protections into the design of the technology. Although this approach originates from the field of engineering, a number of privacy regulators around the world have adopted this idea to regulate and set guidelines for not only information technologies but also for business practices and other types of networked infrastructures. One of the most influential formulations of this approach was developed by the former Information and Privacy Commissioner of Ontario Ann Cavoukian (2009). Her seven foundational Principles of Privacy by Design, which are based on FIPPs, are as follows:

1. *Proactive not reactive; preventative not remedial*: Privacy risks should be anticipated and addressed early in the design phase. Rather than having to react to data breaches, designers should attempt to prevent data breaches from happening in the first place.
2. *Privacy as the default setting*: Privacy should be ensured and automatically protected even if an individual does not do anything.
3. *Privacy embedded into design*: Privacy should be incorporated in the infrastructure of systems and business practices.
4. *Full functionality—positive-sum, not zero-sum*: There should be no trade-offs between privacy and security, and all parties can and should be accommodated.
5. *End-to-end security—full lifecycle protection*: Privacy should be incorporated throughout the lifecycle of a system from start to finish.
6. *Visibility and transparency*: Data operations should remain open to all stakeholders. Operations should also be subject to independent verification.
7. *Respect for user privacy*: Developers and operators should keep the interests of the individual at the highest level of importance.

The second principal, privacy by default, is sometimes considered separately from privacy by design, but the two ideas are highly entwined with one another. As is evident, many of these principles align with FIPPs but are geared towards considering privacy concerns at the upstream phase of system development. Similar to FIPPs, many organizations have utilized these principles in their privacy policies and guidelines. For example, Article 25 of the GDPR obligates data processors to observe privacy by design and privacy by default (European Commission 2016). Because engineers are still in the process of figuring out the full capabilities of new technologies, almost all best practices and recommendations suggest privacy by design as a possible solution to mitigating privacy breaches.

Aside from influencing regulators, the idea of privacy by design has also been growing in popularity within engineering circles. Background research for this study, which included a review of articles on privacy by design ideas for smart meters in the Institute of Electrical and Electronics Engineers (IEEE) online database, found that the number of published articles on the topic grew from six in 2010 to eighty-three in 2017. These articles not only discuss how to prevent privacy breaches for smart meters (e.g. Efthymiou and Kalogridis 2010) but also how to detect privacy breaches or energy theft (e.g. Salinas and Li 2016) and how to measure the tradeoff between privacy and efficiency (e.g. Eibl and Engel 2015). The rising popularity of these topics suggests that privacy as a principle has become a growing concern for engineers and that perhaps engineers are anticipating stricter regulation or are trying to meet the regulatory standards in different areas of the world.

*Contextual Integrity*

In contrast to FIPPs and the principles of privacy by design, the idea of contextual integrity, which has been developed primarily by Nissenbaum (2010, 2018), takes a more flexible approach to setting the privacy standards for situations in which data transfers take place. Rather than having a single, universal set of privacy standards, the idea of contextual integrity assumes that privacy standards should be tailored to the particular context in which they would apply. Under this framework, privacy standards should be shaped by four main factors:

1. The context, or the social backdrop in which the data transfer takes place, such as health care, finance, or the university;
2. The actors, who include the subject of the data, the sender of the data, and the recipient of the data;
3. The attributes or information type, such as a patient’s medical condition in a health context or grades in an education setting; and
4. The transmission principles, or the societal norms, rules, or constraints under which a transfer of information ought to (or ought not to) occur. These principles are highly dependent on the context. For example, the transmission principle of confidentiality means that any data shared with the recipient should remain private. In contrast, the transmission principle of reciprocity defines a bidirectional flow of information, and another type of transmission principle may require a signed waiver.

The framework of contextual integrity promotes identifying these four factors for every information transaction to figure out the acceptable privacy standards for each circumstance. If the expectations of the context are not followed, then contextual integrity has been violated. Not every situation will require the same set of principles, and the contextual integrity approach allows for the fact that norms can change over time.

 Instead of having a universal standard across industries, Nissenbaum (2018) argues that experts in their respective contexts (e.g. healthcare, automobile industry, education, etc.) are in the best position to develop these standards. Difficulties arise when new and unprecedented situations appear. In these instances, Nissenbaum suggests that privacy regulators should study how the new situation influences the various interests of relevant actors, ask whether the changes are fair and just, and finally consider the values and purposes specific to the context. In one context, the value of safety might be more prominent while in another context the value of privacy may be more important. Thus, Nissenbaum argues that regulators should understand context as a dynamic social arena rather than as a type of technology or industry. One might argue that the idea of contextual integrity might be viewed as opposed to efforts to create unified, general privacy standards, such as the European privacy standards. If one interprets the concept of contextual integrity to apply also to cultural contexts, then it would suggest that harmonization efforts would need to be attuned to different norms and expectations of privacy in different countries.

*Summary*

In summary, FIPPs and the Principles of Privacy by Design provide two of the most prominent approaches to privacy principles. They are utilized in most of the privacy regulations around the world, and many of these principles are apparent in the privacy regulations that are discussed in the next section. In contrast to these two sets of standards, the more recent idea of contextual integrity offers a relatively flexible and context-specific approach to setting privacy protection. To some degree, the idea of contextual integrity reflects actual policy practices, which have tended to develop different standards and guidelines for privacy in different settings (e.g., telecommunications, medical records, and Internet usage).

**Privacy and Regulation for Smart Meters and CAVs in the U.S.**

In the U.S., privacy laws are imposed at both the federal and the state levels. Most privacy laws, whether at the federal or state level, apply to public-sector agencies, although a number of regulations do target private organizations in specific industry sectors (Bennet 2008). The Fourth Amendment of the U.S. Constitution states that people have the right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” without a warrant. After the 1979 *Smith v. Maryland* case, the U.S. Supreme Court ruled that the Fourth Amendment does not apply if data are willingly revealed to third parties, which became known as the “third-party doctrine.” Compared to the Fourth Amendment, the Federal Privacy Act of 1974 more explicitly regulates the gathering, access, use, and dissemination of personal data by the federal government. This act also outlines the FIPPs for federal agencies, but it does not directly apply to the private sector.

In addition to these more general privacy laws, the U.S. has some federal privacy laws that specifically pertain to electronic technologies. The Right to Financial Privacy Act of 1978 prohibits the government from obtaining an individual’s financial records without appropriate authorization, and the Electronic Communications Privacy Act of 1986 limits the government’s use of wiretaps on telephones and computers and protects the privacy of communications through email and telephone conversations. Title II of the Electronic Communications Privacy Act, also known as the Stored Communications Act, extended this protection to any data stored electronically. Similarly, the Computer Fraud and Abuse Act of 1986 prevents the intentional accessing of a computer without authorization. In practice, this measure also applies to cellphones and some other digital technologies. Finally, the Video Privacy Protection Act of 1988 prohibits service providers from disclosing video rental information for any reason outside of ordinary business.

The U.S. does not have a single “privacy commissioner” who oversees all issues related to privacy; instead, in a pattern consistent with the contextual integrity approach, there are separate agencies that govern privacy based on the type of industry or sector. For example, the U.S. Department of Health and Human Services’ Office for Civil Rights enforces privacy regulation in the health industry, and the Department of Education’s Family Policy Compliance Office does similar work in the field of education. The authority overseeing the data protection of consumers is the Federal Trade Commission (FTC), which was established by the FTC Act of 1914 to oversee commerce. Section 5 of the FTC Act prohibits unfair or deceptive trade practices that cause harm to consumers, and the FTC has utilized this particular directive to enforce data security standards and consumer privacy regulations. There are ample examples in recent times of the FTC pursuing companies, such as Google and AT&T, for data security breaches or data privacy lapses on the basis of this regulation (Pfeifle 2015, Weinstein 2013).

Differences across states provide another source of contextual variation in privacy protection. California has one of the most progressive privacy regulations in the country, and the state continues to strengthen its protections. For example, a 2013 law in California (Assembly Bill No. 1274) prohibits utility companies as well as any related businesses that handle the collected data from sharing these information to third parties without the customers’ consent. More recently, California passed the Consumer Privacy Act of 2018, which is considered a “landmark policy constituting the most stringent data protection regime in the United States” (Ghosh 2018). The act outlines four basic rights that consumers have over their personal information: the right to know what information is collected about them; the right to “opt out” of allowing businesses to sell their personal information to third parties; the right to have businesses delete their personal information, with exceptions; and the right to receive equal service and pricing from a business even if they do exercise their privacy rights (California Assembly Bill No. 375). The scope of entities that must comply with the act includes for-profit businesses that collect California residents’ personal information and have an annual gross revenue of over $25 million, any companies that handle the personal information of fifty thousand or more Californian residents, and all businesses that receive fifty percent or more of their annual revenues from selling California residents’ personal information. Experts expect that this law will have wide-reaching effects outside of California because many companies often handle Californian data (Matthews and Bowman 2018).

In sum, general privacy regulation in the U.S. tends to be divided by industry, and the stringency and scope varies from one state to another. Usually these regulations are developed in response to circumstances which require the creation of these legislations. A handful of federal laws provides general data and privacy protection, but regulation for specific sectors may vary widely at the individual state level, with California often having the strongest data protections in the country.

*Smart Meters*

In the U.S., state-level public utility commissions regulate utility companies and therefore smart meters. When utility companies first began installing smart meters, these new devices were essentially unregulated (Baumgart 2017). All of the general privacy regulations discussed above (i.e. the Fourth Amendment, the Federal Privacy Act of 1974, the Electronic Communications Privacy Act, and the FTC Act) may still apply to protecting smart meter data (Murrill, Liu, and Thompson II 2012; National Institute of Standards and Technology (NIST) 2014). For example, governments are allowed to use data gathered by utilities to pursue a criminal investigation without a warrant under the Fourth Amendment. However, these laws leave certain privacy questions related to smart meters unresolved—such as the extent to which Fourth Amendment protections apply to private information collected by utility companies.

The Energy Independence and Security Act of 2007 is the first federal regulation in the U.S. that specifically relates to smart meters (Gallagher 2009). Although the act generally seeks to improve energy efficiency and the availability of renewable energy, it also gives NIST the “primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems” (Title XIII, Section 1305). In other words, NIST is tasked with developing standards for the smart meter’s two-way communication system, which is integral to privacy and data protection. NIST updated its *Framework and Roadmap for Smart Grid Interoperability Standards* as well as its *Guidelines for Smart Grid Cybersecurity* in 2014. Chapter five of the latter document particularly discusses privacy and the smart grid, although NIST states that the document “does not prescribe public policy with respect to privacy issues [nor does it] represent legal opinions, but rather was developed to explore privacy concerns, and provide associated recommendations for addressing them” (NIST 2014: 1). As such, the document presents a review of the existing, recommended privacy mitigation tools, including FIPPs and privacy by design principles, as well as some existing design solutions, such as those dealing with cryptographic encryption. The document also broadly recommends that organizations should establish privacy breach notice practices; establish procedures for smart grid consumers to challenge the organization’s compliance as well as their actual privacy practices; and perform regular privacy impact assessments (NIST 2014).

At the state level, privacy regulation of smart meters varies widely by location. As with privacy regulations more generally, California has the most advanced regulations for the privacy of smart meters. The state’s 2011 law (California Senate Bill No. 1476) prohibits utilities from sharing, disclosing, selling, or otherwise making accessible to third parties a customer’s data without the consent of the customer. The law required utilities to use “reasonable security procedures and practices” to protect these data. In 2014, the state expanded the earlier smart meter privacy law by putting the same restrictions on any businesses that handle smart meter data, such as internet service providers and financial institutions (California Assembly Bill No. 1274). Along with these laws, California is also one of only a handful of states that has allowed an opt-out program, which allows customers to retain, or return to, an analog meter for a certain fee.

*CAVs*

 Because CAVs are still an emerging technology, very few laws specifically related to privacy and CAVs have been passed at either the federal or state levels (Jones 2017). Again, the Fourth Amendment, Electronic Communications Privacy Act, and the other general privacy laws mentioned above apply to protecting the privacy of data gathered by CAVs (Colbert 2018, Jones 2017). The Driver’s Privacy Protection Act of 1994, which protects the personal information stored by state motor vehicle departments, is more specific to vehicles, but the most relevant, existing law for autonomous vehicles is the Driver’s Privacy Protection Act of 2015, which outlines the ownership of data that is captured by monitoring devices called “event data recorders” (EDR). Although this act is an important step towards protecting CAV data, the act only applies to EDRs, which records specific information before or during a crash event. Many CAVs are capable of gathering much more detailed information.

Several bills have been proposed to investigate the security and privacy of CAVs, including the Security and Privacy in Your Car Act, the Security and Privacy of Your Car Study Act, and the Autonomous Vehicle Privacy Protection Act of 2015; however, no federal laws have yet been passed to protect the privacy and cybersecurity of CAVs (Ramos 2016). The National Highway Traffic Safety Administration (NHTSA), which is part of the Department of Transportation (DOT), is in charge of governing the safety of passenger vehicles, but the FTC has the primary responsibility of protecting consumer’s privacy and personal data. As such, the two departments often work together to discuss privacy regulation concerning vehicles, including CAVs. To date, the NHTSA and the FTC have only published guidelines, rather than regulations, to help states to create their own protections. For example, the 2017 *Automated Driving Systems 2.0: A Vision for Safety* provides “voluntary guidance” that lists some best practices, and a 2016 policy by the DOT includes a 15-point safety assessment for the testing and deployment of CAVs by manufacturers and developers. These guidelines focus primarily on safety concerns and barely mentions privacy. In the 2017 document, discussions of privacy is relegated to two brief mentions that the DOT encourages the protection of consumer privacy and two other, similar sentences in the footnotes. Even the section on data recording focuses more on gaining information about crashes than on the issue of privacy (DOT and NIST 2017).

The Federal Communications Commission (FCC), which “regulates interstate and international communications by radio, television, wire, satellite, and cable,” may also play a relevant role in protecting CAV data (Jones 2017). Section 222 of the Communications Act tasks the FCC to protect the confidentially of proprietary information gathered by telecommunication carriers. This measure may apply to broadband internet, which could affect some CAVs. Currently, questions still remain about how to regulate and who will have the final authority for regulating the security and privacy of CAVs.

At the state level, regulations concerning CAVs again vary but are also generally very nascent. California and a few other states have passed legislation and regulations that allow the testing of autonomous vehicles, but only Nevada has measures regulating the implementation of autonomous vehicle technology on its roads (Ramos 2016). Seventeen states as of 2017 have some statute that protects EDR data, but no state laws have addressed the security and privacy issues of CAVs (Norton Rose Fulbright 2017). Some legal experts suggest that California’s Online Privacy Protection Act, which protects privacy for consumer websites, may partly apply to CAVs, but they acknowledge that the portability of this act would still leave some regulatory gaps (Colbert 2018). In 2014, a bill in the California legislature was proposed to give consumers control over the data collected by CAVs, but the measure did not pass.

Aside from federal and state governments, industry actors are also working to protect CAV data. A group of automakers has developed the Automotive Consumer Privacy Protection Principles, which seeks to protect customer privacy in the development of vehicles. These principles overlap with FIPPs and include transparency, choice, respect for context, data minimization, de-identification and retention, data security, integrity and access, and accountability (Alliance of Automobile Manufacturers and the Association of Global Automakers 2014). These guidelines are voluntary, but twenty automakers have pledged to meet or exceed these commitments no later than in their model year 2017 vehicles.

**Privacy and Regulation for Smart Meters and CAVs in the E.U.**

In contrast to the U.S., the regulatory structure governing privacy in the E.U. is more centralized. Privacy is recognized as an important right by the European Convention on Human Rights as well as by the E.U. Charter of Fundament Rights, which states that “everyone has the right to respect for his or her private and family life, home and communications” (European Parliament, the European Council and the European Commission 2012: Article 7). Article 8, titled “Protection of personal data,” of the Charter of Fundamental Rights also states that “everyone has the right to the protection of personal data concerning him or her” (European Parliament, the European Council and the European Commission 2012). Privacy regulations and guidelines in the E.U. are issued at the supranational as well as at the national level, and recent developments have led to the increasing harmonization of privacy regulation across member nations. In an effort to synchronize European data protection law and allow easier movement of data across member states, the E.U. adopted the Data Protection Directive in 1995. The directive provides guidelines for privacy regulation and calls for each member state to set up a supervisory body to oversee privacy related matters. In 2002, the European Commission expanded the Data Protection Directive by creating the Privacy and Electronic Communications Directive, more commonly known as the ePrivacy Directive, which specifically concerns data protection related to digital technologies (Pohle 2018). These two directives provide complementary guidelines for privacy regulation, and according to the Treaty on the Functioning of the European Union, member states are obligated to transpose these directives into national law.

In 2012, the European Commission decided to create a single policy, known as the General Data Protection Regulation (GDPR), which would be enacted in each of the member states to facilitate cooperation and lower the costs of implementing and enforcing privacy regulations across borders (Pohle 2018). The GDPR supersedes the Data Protection Directive and went into effect in May, 2016, with a two-year transitional period. Member states and relevant companies began compliance with GDPR on May 25, 2018. The European Commission has similarly proposed to update the ePrivacy Directive with a new law called the ePrivacy Regulation; however, the proposed law had not yet been approved as of 2018 (European Commission 2018). In contrast to directives, which member states are obligated to follow by developing national laws, regulations are directly applicable as law for all member states.

The GDPR builds on the earlier directive but has a greater scope, more specific data protection requirements, and harsher penalties for noncompliance. The GDPR applies to all entities that process any E.U. citizens’ data regardless of whether they are in the E.U., or outside the E.U. (European Commission 2016). Moreover, not only private but also public authorities, with the exception of those concerning criminal prosecution and prisons as well as the police or military, must comply with GDPR. Although the GDPR seeks first and foremost to protect the data and privacy of E.U. citizens, the regulation has far-reaching consequences and has led to the gradual harmonization of privacy policies across the world. Given the current, global interconnectedness of data processing systems, this new regulation affects a significant number of organizations across the world. A survey conducted by Vanson Bourne, a market research organization, estimated that about 52 percent of large companies in the U.S. have some type of data on E.U. citizens, which makes them subject to the GDPR (Compuware Corporation 2016). The GDPR details specific rules protecting specific data privacy rights, including the subjects’ right of access, right of data rectification, right to erasure—or the “right to be forgotten”—right to restriction of processing, right to data portability, and the right to object. Companies must be transparent in their communication of these rights. Although these rights align with FIPPs, some of these rights, including the right to erasure, go beyond FIPPs compliance. The cost of noncompliance is a fine of up to twenty million euros or four percent of the company’s global annual turnover.

Because the European Commission, the European Parliament, and the Council of Ministers had disagreements on several issues when the GDPR was being developed, it contains over seventy “opening clauses” that allow member states to adopt more specific data protection rules for certain regulatory areas (Pohle 2018). Moreover, data protection in the E.U. is not limited to the GDPR and its opening clauses. Specific data protection regulations may result from complying with other technical E.U. directives. For example, Germany’s Act on the Digitization of Energy Transition, which sets the minimum technical requirements to ensure data protection and security, was created in part to comply with another E.U. directive concerning energy.

*Smart Meters*

In the E.U., the 2006 Energy Service Directive first introduced the idea of using smart meters to allow consumers to manage their energy usage. In 2009, the Electricity Directive, which is a part of the Third Energy Package or “third legislative package,” stipulates that “at least 80 percent of consumers shall be equipped with intelligent metering systems by 2020” (European Commission 2009). This directive was created to give consumers the right to switch energy providers and to receive energy bills in a correct and timely manner (Knyrim and Trieb 2011). In 2012, the Energy Efficiency Directive sought to expand these earlier provisions and was the first to mention issues of data privacy and security in the installation of smart meters. Article 9 states that “smart meters and data communication must be secure and the privacy of final customers must be in compliance with relevant Union data protection and privacy legislation” (European Commission 2012).

Most recently, the 2016 Clean Energy Package proposed to recast the Electricity Directive to better protect electricity customers and give them more power over their billing information (Erbach 2018). Article 20 of the this Directive details seven principles related to the roll-out of smart meters, most of which is concerned with protecting customers’ data (Fratini and Pizza 2018). More specifically, these principles state that data from smart meters should be made easily available to customers; that customers should be notified of the collection and processing of their personal data; and that smart metering systems should comply with relevant E.U. security, data protection, and privacy legislations, which refers to the GDPR. This means that the GDPR grants the same rights (e.g. right of access, right of data rectification, right to erasure, etc.) and protections to smart meter customers as for customers in other sectors.

*CAVs*

The first E.U. legislation pertaining to CAVs was the 2010 Directive on Intelligent Transport Systems, which created a framework to coordinate the introduction of CAVs in the E.U. (Reibach 2016); however, the directive only makes references to general data protection rules and does not establish specific regulation for data protection in CAVs. Generally, CAVs in the E.U. must now comply with GDPR, but the problem lies in how CAVs should comply with the E.U.-wide privacy regulation (Yaros and Nishikawa 2017). One of the biggest issues is how to define personal data. Any data that can be used, either directly or indirectly, to identify an individual or be traced back to an individual is considered personal data. Thus, personal data include the drivers’ name, contact details, location data, journey history, mileage and speed data, as well as any recorded sounds, footage, or data gathered from the CAV’s environment. These data may be valuable to certain organizations, such as insurance companies, advertisers, vehicle manufacturers, or law enforcement; however, disagreements still exist over which data may be transferred automatically to which of these various entities either under the legal permit under the GDPR or by the basis of consent. In fact, no current opening clause in the GDPR refers to research on CAVs; thus, data collected by CAV test drives are technically violations of GDPR.

Another question is how these entities should provide privacy notices to users of CAVS. The GDPR requires companies to notify in a clear manner the purposes for and method of using people’s personal data so that individual’s consent is freely given, able to be easily withdrawn, auditable, and verifiable (Colbert 2018). The right to withdraw or delete data may be challenging when working with artificial intelligence. Moreover, the GDPR’s data minimization principle, which directs companies to gather as little personal data as possible, may affect CAVs because the core machine learning technology of these vehicles often relies on the bulk gathering of information (Lavery and McMahon 2017). At minimum, the principle necessitates giving drivers the ability to switch off data transmissions that are not necessary for the function of the vehicle.

The Resolution on Data Protection in Automated and Connected Vehicles developed during the 2017 International Conference of Data Protection Commissioners encourages relevant entities to give people “comprehensive information as to what data is collected and processed in the deployment of connected vehicles, for what purposes and by whom” (p. 3). Because these technologies are still in development, legal experts suggest that all relevant parties, including CAV manufacturers and regulators, should work together to carefully outline agreements that clearly enumerate each party’s respective obligations with respect to issues such as the ownership of collected data and the use and protection of personal data. Another possible solution is adopting data protection by design or by default, which, as is suggested by GDPR, may include anonymization and pseudonymization. These two techniques can blur the line between what is considered personal data and technical data, the latter of which does not fall under GDPR, and may help address both the notice and data minimization problems (Storing 2017). As of April 2018, the E.U. Emergency Call Regulation requires that every new vehicle registered in the E.U. must be equipped with “eCall” technology that would allow emergency services to remotely gather information about a vehicle in an accident (European Commission 2015). Information includes the vehicle’s exact location, the incident time and direction of travel, and the general state of the driver’s health. The measure was created to reduce emergency response times and reduce fatalities in car accidents; however, the mandatory wireless technology provides another challenge for privacy protection (Ammann 2016).

**Discussion: Comparison of the U.S and the EU**

This review finds significant differences in data protection and privacy regulations and guidelines between the U.S. and the E.U. Differences include the structure, regulatory reach, and penalties for noncompliance. Privacy protection also differs between smart meters and CAVs, with CAVs often having less defined regulations. Table 1 summarizes the differences in general regulatory structure between the U.S. and the E.U., and Table 2 gives a summary of the privacy regulation concerning smart meters and CAVs in each locale.

Recent developments in the E.U. have led privacy regulation to become increasingly harmonized among member states. The GDPR provides a single guideline for a broad range of organizations across multiple sectors; thus, the general privacy benchmarks for smart meters and CAVs in the E.U. are very similar. Although there are still substantial unresolved issues, such as how to enforce the privacy regulation, the main problem for regulators and technology developers becomes how companies who work with these technologies should comply with the central privacy regulation. In contrast to the E.U., the state of privacy law in the U.S. has often been called a “patchwork” of data protection (Pizzi 2017). Although federal privacy regulation exists, different industries have different authorities in charge of regulating privacy. Moreover, privacy regulation can differ significantly across states. This patchwork structure is consistent with a contextual integrity approach to privacy protection, in which each state or industry can develop its own set of transmission principles based on the context, actors, information type, and set of values that the relevant actors identify to be important. In this perspective, differences between state regulations can be viewed as differences in values and contexts between people who live in different states—although the overall lack of regulation in some cases may be more due to the novelty of these technologies. For example, California is where many technology companies, such as Uber and Google’s Waymo, test their CAVs; thus, CAV regulation in California tends to be the most progressive in the U.S. (Karsten and West 2018).

Currently, no federal privacy regulation in the U.S. is comparable to the GDPR in terms of either reach or strength of protection. As previously mentioned, the GDPR covers all entities, whether private or public, that handle the data of any E.U. citizen. In contrast, many of the federal and state privacy regulation in the U.S. only apply to government actors, and regulation covering certain private entities, such as utility companies, has been developed separately. At the state level, California’s new Consumer Privacy Act may be the closest to GDPR; however, the latter gives more comprehensive protections and imposes more requirements than the Californian law (Matthews and Bowman 2018). For example, California’s law does not include the right to be forgotten or the right to rectification, which are included in the GDPR. Moreover, the E.U. law outlines specific procedures for a broad array of situations that are not considered in the California law, such as how to notify individuals and regulators of data breach notifications and how to handle cross-border data transfers. Another major difference is that the GPDR requires consumers to “opt in,” in other words to give consent before companies can use personal information, whereas California’s law requires companies to give consumers an “opt-out” option to prevent companies from selling their data. The penalties outlined for the E.U. are also potentially much harsher than in the U.S., although the enforcement of such penalties has yet to be practically established.

The history of privacy regulations in the E.U. and the U.S. suggests differences in how regulatory bodies in both places approach regulation. In the U.S., regulation tends to be reactionary, or as a response to an event, whereas regulation tends to be precautionary in the E.U. For example, U.S.’s Video Privacy Protection Act of 1988 was enacted after Supreme Court nominee Robert Bork’s video rental records were published in a newspaper. Similarly, U.S.’s Financial Privacy Act of 1978 was developed as a response to the U.S. Supreme Court’s 1976 ruling in the *United States v. Miller*, which stated that financial records were owned by the financial institution rather than the customer. In comparison, regulators in the E.U. tend to prioritize safety in unknown situations and place strict restrictions on new technologies. For example, this precautionary approach has been well-document in the case of E.U.’s approach to genetically modified organisms (GMOs), which is highly regulated by the European Food Safety Authority (Guehlstorf and Hallstrom 2005). The two different approaches suggest that people in the U.S. and the E.U. hold different underlying ethical values, which is then reflected in their regulations, including those related to privacy. In the U.S., over-regulation is often a major concern, especially for conservatives. As Scribner (2014) states, “If automated vehicles are demonstrated to be significantly safer than manually driven vehicles, any misstep, convoluted law, or burdensome rule that leads to unnecessary higher costs or delays translates to increased injury and death” (p. 11). Thus, although the E.U. has more comprehensive privacy protections than the U.S., a universal privacy regulation like the GDPR may not be realistically transferable to the U.S. Nevertheless, valuable insights into privacy regulation may still be gathered from the examples of either places.

**Conclusion**

The current regulatory landscape suggests that the E.U. and the U.S. are approaching the issue of privacy for smart meters and CAVs in two distinct ways. However, two factors are likely to drive further harmonization: the use of both smart meters and CAVs in global markets and the difficulty of applying privacy regulations to E.U. citizens only when information is embedded in global networks. Within the U.S., market considerations will also likely drive harmonization across state governments. For example, the problem with tackling the regulation of CAVs at the individual state level is that these technologies will more than likely cross state borders. As Pizzi (2017) remarks, “Privacy in regard to connected vehicles appears ill-suited to state-by-state regulation, given that motor vehicles are by definition mobile, and manufacturers cannot be expected to design different vehicles for different states” (p. 1).

At present the strongest regulatory guidelines for privacy for emerging information-based technologies are the E.U.’s GDPR and California’s Consumer Privacy Act. Neither has been fully tested and implemented as of 2018, and companies and engineers are still trying to figure out how to comply with them. Some of the guidance also applies directly to companies, which must think about how to integrate privacy concerns into upstream design processes. FIPPs is embedded into the GDPR; however, the Californian privacy regulation does not fully align with the principles and fails to address the principles of data minimization, of use limitation, and of data quality and integrity. Instead, California’s privacy regulation focuses more on the principles of transparency, purpose specification, and individual participation, which are all related to granting consumers’ access to information and the ability to give consent. Unlike with GDPR, consent is assumed and the act allows consumers to opt out. Similarly, the GDPR explicitly discusses the idea of privacy by design, whereas in the U.S. the idea of privacy by design primarily exists in guidelines and are not embedded in official regulation. If the direction of privacy regulation is towards stronger consumer protection, then the GDPR currently sets the highest standard.

At the same time, both the GDPR and the Californian measure in some cases go beyond FIPPs and the Principles of Privacy by Design. Both measures give consumers the right to delete their information, which is not stated in either set of principles, and the California privacy act protects consumers’ right to receive equal service and pricing even if they exercise their privacy rights. This principle of equality or fairness is not considered in either FIPPs or the Principles of Privacy by Design. Thus, although both sets of principles may provide useful, common starting points for privacy regulators and technology developers, other approaches to privacy may be also useful to consider, and ethical principles that are implied by regulations can be brought back into the discussion of improved data protection. Likewise, the experience of technology-specific regulation, such as for smart meters and CAVs, can be brought together with the idea of contextual integrity to enable the discussion of industry-specific privacy principles. Being aware of differences in context and people’s values may lead to better-fitting policies. Regulators and developers should be aware of these various approaches to privacy regulation to help identify gaps in data protection

Table 1: Comparison of E.U. and U.S. Privacy Regulatory Structures

|  |  |  |
| --- | --- | --- |
|   | E.U. | U.S. |
| Regulatory Source | Supranational and national | Federal and state |
| Major Regulatory Authority(ies) | European Commission | Depends on industry or sector; e.g. Federal Trade Commission (FTC) for consumer privacy |
| Regulatory Approach | Precautionary | Reactionary |
| Organizational Coverage | All organizations that handle the data of E.U. citizens | Mainly public-sector plus some specific private industry sectors |
| Major E.U.-wide/ Federal Privacy Laws | European Convention on Human RightsEU Charter of Fundamental Rights1995 E.U. Data Protection Directive (replaced by GDPR)2002 Privacy and Electronic Communications Directive (ePrivacy Directive)2018 General Data Protection Regulation (GDPR)ePrivacy Regulation (proposed) | 4th AmendmentFederal Privacy Act of 1974Federal Trade Commission Act of 1914, Section 5Electronic Communications Privacy Act of 1986 (ECPA) Title II of ECPA: Stored Communications ActComputer Fraud and Abuse Act of 1986 |

Table 2: Privacy Laws that More Specifically Apply to Smart Meters and CAVs

|  |  |  |
| --- | --- | --- |
|   | E.U. | U.S. |
| Smart Meters | Major regulatory authority(ies) | European Commission | State-level Public Utility CommissionsNational Institute of Standards and Technology (NIST) |
|   | Major E.U.-wide/Federal Privacy Laws | GDPR2006 Energy Service Directive2009 Electricity Directive2012 Energy Efficiency Directive2016 Clean Energy Package | The Energy Independence and Security Act of 2007NIST has developed some guidelines |
| CAVs | Major regulatory authority(ies) | European Commission | National Highway Traffic Safety Administration (NHTSA)FTC |
|   | Major E.U.-wide/Federal Privacy Laws | 2010 Directive on Intelligent Transport SystemsGDPR2015 Emergency Call Regulation (eCall) | Driver’s Privacy Protection Act of 2015Not yet well developed; have suggested guidelines  |

**References**

Alliance of Automobile Manufacturers Inc. & Association of Global Automakers Inc. (2014). Consumer privacy protection principles: privacy principles for vehicle technologies and services. Auto Alliance, November 12. <https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf>. Accessed 15 Dec. 2018.

Ammann, T. (2016). Michael–darf ich fahren? Das Automobil aus IT-Sicherheitsrechtlicher Perspektive. In Jürgen T. (Ed.), *Smart world –smart law?–weltweite netze mit regionaler regulierung* (p. 299-308). Edewecht: Olwir, Oldenburger Verlag für Wirtschaft, Informatik und Recht.

Bagloee, S. A., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous vehicles: challenges, opportunities, and future implications for transportation policies. *Journal of Modern Transportation* 24(4): 284-303.

Baumgart, M. (2017). A (legal) challenge to privacy: on the implementation of smart meters in the E.U. and the U.S. *Renewable Energy Law & Policy Review* 8(1): 19-29.

Bennet, C. J. (2008). *The privacy advocates: resisting the spread of surveillance*. Cambridge: MIT Press.

Bonneau, V., Yi, H, Probst, L., Pedersen, B., & Lonkeu, O. K. (2017). Autonomous cars: a big opportunity for European industry. European Commission, Digital Transformation Monitor, January. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM\_Autonomous%20cars%20v1.pdf. Accessed 15 Dec. 2018.

California Assembly Bill No. 1274, chapter 597, an act to add Title 1.81.4 (commencing with Section 1798.98) to Part 4 of Division 3 of the Civil Code, relating to privacy. (2013). California Legislative Information. <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1274>. Accessed 15 Dec. 2018.

 California Assembly Bill No. 375, chapter 55, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy. (2018). California Legislative Information. <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>. Accessed 15 Dec. 2018.

California Public Utilities Commission. (2011). Decision Modifying Pacific Gas and Electric Company's Smartmeter Program to Include an Opt-0ut Option. [http://docs.cpuc.ca.gov/PUBLISHED/AGENDA\_DECISION/158309.htm](http://docs.cpuc.ca.gov/PUBLISHED/AGENDA_DECISION/158309.htm.%20Accessed%2015%20Dec.%202018). Accessed 15 Dec. 2018.

California Senate Bill No. 1476, chapter 497, an act to add Chapter 5 (commencing with Section 8380) to Division 4.1 of, and to repeal Section 393 of, the Public Utilities Code, relating to public utilities. (2010). California Legislative Information. <http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200920100SB1476>. Accessed 15 Dec. 2018.

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information & Privacy Commissioner, Ontario, Canada. <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>. Accessed 15 Dec. 2018.

Colbert, C. (2018). Privacy under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles. 7th annual conference on robotics, law and policy.

Compuware Corporation. (2016). Unprepared for GDPR? A research report on the state of enterprise readiness for the EU’s New PII Mandates. Compuware.

Dahn, S. (2014). Fair information practice principles (FIPPs). Department of Homeland Security, Privacy Office. <https://www.dhs.gov/publication/fair-information-practice-principles-fipps>. Accessed 15 Dec. 2018.

Department of Transportation and the National Highway Traffic Safety Administration. (2017). Automated driving systems: a vision for safety 2.0. <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf>. Accessed 15 Dec. 2018.

Edmonds, E. (2018). AAA: American trust in autonomous vehicles slips. American Automobile Association. <https://newsroom.aaa.com/2018/05/aaa-american-trust-autonomous-vehicles-slips/>. Accessed 15 Dec. 2018.

Efthymiou, C. & Kalogridis, G. (2010). Smart grid privacy via anonymization of smart metering data. In *First IEEE International Conference on Smart Grid Communications* (pp. 238–243). IEEE.

Eibl, G. and Engel, D. (2015). Influence of data granularity on smart meter privacy. *IEEE Transactions on Smart Grid* 6(2): 930-939.

Erbach, G. (2018). Briefing EU legislation in progress: common rules for the internal electricity market. European Parliament. [http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/595924/EPRS\_BRI(2017)595924\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/595924/EPRS_BRI%282017%29595924_EN.pdf). Accessed 15 Dec. 2018.

European Commission. (2009). Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC. *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0072&from=EN>. Accessed 15 Dec. 2018.

---. (2012). Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC. *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012L0027&from=EN>. Accessed 15 Dec. 2018.

---. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

---. (2015). eCall in all new cars from April 2018. European Commission. <https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018>. Accessed 15 Dec. 2018.

---. (2018). Proposal for an ePrivacy Regulation. European Commission. <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>. Accessed 15 Dec. 2018.

European Parliament, the European Council and the European Commission. (2012). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>. Accessed 15 Dec. 2018.

Flipse, S. M. & Puylaert, S. (2018). Organizing a collaborative development of technological design requirements using a constructive dialogue on value profiles: A case in automated vehicle development. *Science and Engineering Ethics* 24: 49-72.

Fratini, A. and Pizza, G. (2018). Data protection and smart meters: the GDPR and the ‘winter package’ of EU clean energy law. EU Law Analysis. <http://eulawanalysis.blogspot.com/2018/03/data-protection-and-smart-meters-gdpr.html>. Accessed 15 Dec. 2018.

Gallagher, P. (2009). Progress on smart grid initiatives authorized in the Energy Independence and Security Act of 2007. National Institute of Standards and Technology. <https://www.nist.gov/speech-testimony/progress-smart-grid-initiatives-authorized-energy-independence-and-security-act>. Accessed 15 Dec. 2018.

Ghosh, D. (2018). What you need to know about California’s new data privacy law. *Harvard Business Review* July 11. <https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law>. Accessed 15 Dec. 2018.

Gogoll, J. & Müller, J. F. (2017). Autonomous cars: in favor of a mandatory ethics setting. *Science and Engineering* Ethics 23: 681-700.

Granville, K. (2018). Facebook and Cambridge Analytica: what you need to know as fallout widens. *New York Times*, March 19. <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>. Accessed 15 Dec. 2018.

Greenberg, A. (2015). Hackers remotely kill a jeep on the highway—with me in it. *Wired*, July 21. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>. Accessed 15 Dec. 2018.

Guehlstorf, N. P. and Hallstrom, L. K. (2005). The role of culture in risk regulations: a comparative case study of genetically modified corn in the United States of America and the European Union. *Environmental Science & Policy* 8(4): 327-342.

Hess, D. J. (2014). Smart meters and public acceptance: comparative analysis and governance implications. *Health, Risk & Society* 16(3): 243-258.

Hevelke, A. & Nida-Rümelin, J. (2015). Responsibility for crashes of autonomous vehicles: an ethical analysis. *Science and Engineering Ethics* 21: 619-630.

International Conference of Data Protection and Privacy Commissioners. (2017). Resolution on data protection in automated and connected vehicles. <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf>. Accessed 15 Dec. 2018.

Jones, A. (2017). Autonomous cars: navigating the patchwork of data privacy laws that could Impact the Industry. *Catholic University Journal of Law and Technology* 25(1): 180-204.

Karsten, J. & West, D. (2018). The state of self-driving car laws across the U.S. Brookings. <https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/>. Accessed 15 Dec. 2018.

Knyrim, R. & Trieb, G. (2011). Smart metering under EU data protection law. *International Data Privacy Law* 1(2): 121-128.

Lavery, P. & McMahon, D. (2017). Driverless cars—mapping the privacy issues. McCann FitzGerald. <https://www.mccannfitzgerald.com/knowledge/privacy/driverless-cars-mapping-the-privacy-issues>. Accessed 15 Dec. 2018.

Mathews, K. & Bowman, C. M. (2018). The California Consumer Privacy Act of 2018. Proskauer: Privacy Law Blog. <https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/>. Accessed 15 Dec. 2018.

McDaniel, P. & McLaughlin, S. (2009). Security and privacy challenges in smart grids. *Institute of Electrical and Electronics Engineers Security and Privacy* 7(3): 75-77.

Mladenovic, M. N. & McPherson, T. (2016). Engineering social justice into traffic control for self-driving vehicles? *Science and Engineering Ethics* 22: 1131-1149.

Murrill, B J., Liu, E. C., & Thompson II, R. M. (2012). Smart meter data: privacy and cybersecurity. Congressional Research Service Report for Congress. <http://www.smartmetereducationnetwork.com/uploads/privacy/Congressional%20Research%20Services%20Smart%20Meter%20Data--%20Privacy%20and%20Security.pdf>. Accessed 15 Dec. 2018.

National Institute of Standards and Technology. (2014). Guidelines for smart grid cybersecurity. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>. Accessed 15 Dec. 2018.

Nissenbaum, H. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford University Press: Stanford, CA.

---. (2018). Respecting context to protect privacy: why meaning matters. *Science and Engineering Ethics* 24: 831-852.

Norton Rose Fulbright. (2017). The privacy implications of autonomous vehicles. Norton Rose Fulbright, Data Protection Report. <https://www.dataprotectionreport.com/2017/07/the-privacy-implications-of-autonomous-vehicles/>. Accessed 15 Dec. 2018.

Pfeifle, S. (2015). FCC Fines AT&T $25 m for data privacy lapse; Who will be next? The International Association of Privacy Professionals, April 9. <https://iapp.org/news/a/fcc-fines-at-who-will-be-next/>. Accessed 15 Dec. 2018.

Pizzi, P. J. (2017). Connected cars and automated driving: privacy challenges on wheels. *Defense Counsel Journal* 84(3). <https://www.iadclaw.org/publications-news/defensecounseljournal/connected-cars-and-automated-driving-privacy-challenges-on-wheels>. Accessed 15 Dec. 2018.

Pohle, J. (2018). Data privacy legislation in the EU member states–practical overview. *Computer and Law International Review* 19(5): 97-116, 133-147.

Public Policy Polling. (2018). Aggregate survey results. Consumer Watchdog. <https://www.consumerwatchdog.org/sites/default/files/2018-05/AggregateResults.pdf>. Accessed 15 Dec. 2018.

Ramos, G. (2016). Autonomous vehicles: will the cybersecurity risks be addressed? Bloomberg: Privacy & Security Law Report, October 3. <https://www.squirepattonboggs.com/~/media/files/insights/publications/2016/10/autonomous-vehicles-will-the-cybersecurity-risks-be-addressed/gretchenramos-bloombergbna-15pvlr1932.pdf>. Accessed 15 Dec. 2018.

Reibach, B. (2016). Smart Cars - Smart Privacy Law? Regionale Datenschutzregulierung des vernetzten Kfz in EU und USA. In Jürgen Taeger (Ed.) *Smart World – Smart Law? – Weltweite Netze mit regionaler Regulierung* (p. 13-27). Edewecht: Olwir, Oldenburger Verlag für Wirtschaft, Informatik und Recht.

Salinas, S. A. & Li, P. (2016). Privacy-preserving energy theft detection in microgrids: a state estimation approach. *Institute of Electrical and Electronics Engineers Transactions on Power Systems* 31(2): 883-894.

Scribner, M. (2014). Self-driving regulation: pro-market policies key to automated vehicle innovation. *Competitive Enterprise Institute* 192: 1-14. <https://cei.org/onpoint/self-driving-regulation>. Accessed 15 Dec. 2018.

Stephens, J. C., Wilson, E. J., & Peterson, T. R. (2015). *Smart grid (r)evolution: electric power struggles*. New York: Cambridge University Press.

Storing, M. (2017). What EU legislation says about car data: legal memorandum on connected vehicles and data. Federation Internationale de L’automoile. Osborne Clarke. <https://www.fiaregion1.com/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf>. Accessed 15 Dec. 2018.

Taeger, J. (2017). *Chancen und Risiken von Smart Cams im öffentlichen Raum*. Baden-Baden: Oldenburger Forum der Rechtswissenschaften , Vol. 7.

U.S. Congress. Energy Independence and Security Act of 2007Public Law No: 110-140 (12/19/2007). (2007). <https://www.congress.gov/bill/110th-congress/house-bill/6/text>. Accessed 15 Dec. 2018.

Weinstein, J. (2012). The U.S. Doesn’t Have a National Data Protection Authority? Think Again… The International Association of Privacy Professionals, Oct. 16. <https://iapp.org/news/a/america-doesnt-have-a-national-data-protection-authority-think-again/>. Accessed 15 Dec. 2018.

Yaros, O. & Nishikawa, R. (2017). Connected and autonomous vehicles in Europe: the challenges with using the data they generate. Mayer Brown, July 12. <https://www.mayerbrown.com/files/Publication/d9fa82f6-0cd1-4fdb-beb7-8472ce6e66b3/Presentation/PublicationAttachment/47eb74d6-8e19-4a42-95b4-855d0cf052ab/UPDATE_Connected_and_Autonomous_Vehicles_in_Europe.pdf>. Accessed 15, Dec. 2018.