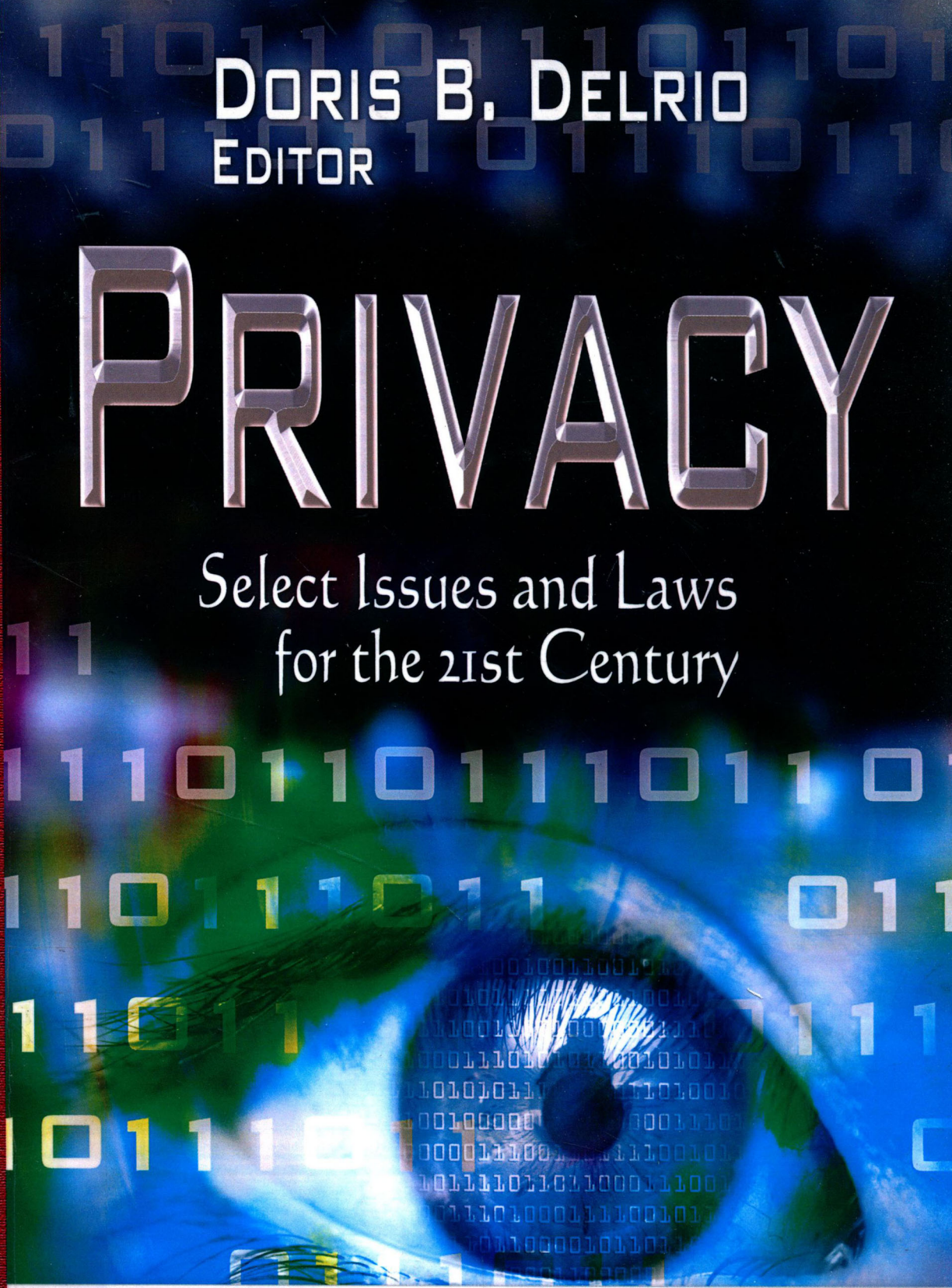
Doris B. Delrio
Editor

Privacy

Select Issues and Laws for the 21st Century



Privacy and Identity Protection

NOVA

PRIVACY AND IDENTITY PROTECTION

PRIVACY

SELECT ISSUES AND LAWS FOR THE 21ST CENTURY

DORIS B. DELRIO
EDITOR

nova publishers
New York

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-62618-429-9

Published by Nova Science Publishers, Inc. † New York

PRIVACY

SELECT ISSUES AND LAWS FOR THE 21ST CENTURY

PRIVACY AND IDENTITY PROTECTION

Additional books in this series can be found on Nova's website under the Series tab.

Additional E-books in this series can be found on Nova's website under the E-book tab.

LAWS AND LEGISLATION

Additional books in this series can be found on Nova's website under the Series tab.

Additional E-books in this series can be found on Nova's website under the E-book tab.

PREFACE

This book is a study of select issues and laws relating to privacy in the 21st century. Topics examined include an overview of federal law governing wiretapping and electronic eavesdropping under the Electronic Communications Privacy Act (ECPA); background and issues related to the USA PATRIOT Act reauthorization on government collection of private information; the United States v. Jones court case involving GPS monitoring, property and privacy; Fourth Amendment implications and legislative responses to drones in domestic surveillance operations; and the privacy and security concerns surrounding smart meter technology.

Chapter 1 – Fueled by stimulus funding in the American Recovery and Reinvestment Act of 2009 (ARRA), electric utilities have accelerated their deployment of smart meters to millions of homes across the United States with help from the Department of Energy's Smart Grid Investment Grant program.

As the meters multiply, so do issues concerning the privacy and security of the data collected by the new technology. This Advanced Metering Infrastructure (AMI) promises to increase energy efficiency, bolster electric power grid reliability, and facilitate demand response, among other benefits. However, to fulfill these ends, smart meters must record near-real time data on consumer electricity usage and transmit the data to utilities over great distances via communications networks that serve the smart grid. Detailed electricity usage data offers a window into the lives of people inside of a home by revealing what individual appliances they are using, and the transmission of the data potentially subjects this information to interception or theft by unauthorized third parties or hackers.

Unforeseen consequences under federal law may result from the installation of smart meters and the communications technologies that accompany them. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It begins with an examination of the constitutional provisions in the Fourth Amendment that may apply to the data. As we progress into the 21st century, access to personal data, including information generated from smart meters, is a new frontier for police investigations. The Fourth Amendment generally requires police to have probable cause to search an area in which a person has a reasonable expectation of privacy.

However, courts have used the third-party doctrine to deny protection to information a customer gives to a business as part of their commercial relationship. This rule is used by police to access bank records, telephone records, and traditional utility records. Nevertheless, there are several core differences between smart meters and the general third-party cases that

may cause concerns about its application. These include concerns expressed by the courts and Congress about the ability of technology to potentially erode individuals' privacy.

If smart meter data and transmissions fall outside of the protection of the Fourth Amendment, they may still be protected from unauthorized disclosure or access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). These statutes, however, would appear to permit law enforcement to access smart meter data for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA), subject to certain conditions. Additionally, an electric utility's privacy and security practices with regard to consumer data may be subject to Section 5 of the Federal Trade Commission Act (FTC Act). The Federal Trade Commission (FTC) has recently focused its consumer protection enforcement on entities that violate their privacy policies or fail to protect data from unauthorized access. This authority could apply to electric utilities in possession of smart meter data, provided that the FTC has statutory jurisdiction over them. General federal privacy safeguards provided under the Federal Privacy Act of 1974 (FPA) protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities.

Chapter 2 – The prospect of drone use inside the United States raises far-reaching issues concerning the extent of government surveillance authority, the value of privacy in the digital age, and the role of Congress in reconciling these issues.

Drones, or unmanned aerial vehicles (UAVs), are aircraft that can fly without an onboard human operator. An unmanned aircraft system (UAS) is the entire system, including the aircraft, digital network, and personnel on the ground. Drones can fly either by remote control or on a predetermined flight path; can be as small as an insect and as large as a traditional jet; can be produced more cheaply than traditional aircraft; and can keep operators out of harm's way. These unmanned aircraft are most commonly known for their operations overseas in tracking down and killing suspected members of Al Qaeda and related organizations. In addition to these missions abroad, drones are being considered for use in domestic surveillance operations, which might include in furtherance of homeland security, crime fighting, disaster relief, immigration control, and environmental monitoring.

Although relatively few drones are currently flown over U.S. soil, the Federal Aviation Administration (FAA) predicts that 30,000 drones will fill the nation's skies in less than 20 years. Congress has played a large role in this expansion. In February 2012, Congress enacted the FAA Modernization and Reform Act (P.L. 112-95), which calls for the FAA to accelerate the integration of unmanned aircraft into the national airspace system by 2015. However, some Members of Congress and the public fear there are insufficient safeguards in place to ensure that drones are not used to spy on American citizens and unduly infringe upon their fundamental privacy. These observers caution that the FAA is primarily charged with ensuring air traffic safety, and is not adequately prepared to handle the issues of privacy and civil liberties raised by drone use.

This report assesses the use of drones under the Fourth Amendment right to be free from unreasonable searches and seizures. The touchstone of the Fourth Amendment is reasonableness. A reviewing court's determination of the reasonableness of drone surveillance would likely be informed by location of the search, the sophistication of the technology used, and society's conception of privacy in an age of rapid technological advancement. While individuals can expect substantial protections against warrantless

government intrusions into their homes, the Fourth Amendment offers less robust restrictions upon government surveillance occurring in public places and perhaps even less in areas immediately outside the home, such as in driveways or backyards. Concomitantly, as technology advances, the contours of what is reasonable under the Fourth Amendment may adjust as people's expectations of privacy evolve.

In the 112th Congress, several measures have been introduced that would restrict the use of drones at home. Senator Rand Paul and Representative Austin Scott introduced the Preserving Freedom from Unwarranted Surveillance Act of 2012 (S. 3287, H.R. 5925), which would require law enforcement to obtain a warrant before using drones for domestic surveillance, subject to several exceptions. Similarly, Representative Ted Poe's Preserving American Privacy Act of 2012 (H.R. 6199) would permit law enforcement to conduct drone surveillance pursuant to a warrant, but only in investigation of a felony.

Chapter 3 – In *United States v. Jones*, 132 S. Ct. 945 (2012), all nine Supreme Court Justices agreed that Jones was *searched* when the police attached a Global Positioning System (GPS) device to the undercarriage of his car and tracked his movements for four weeks. The Court, however, splintered on what constituted the search: the attachment of the device or the long-term monitoring. The majority held that the *attachment* of the GPS device and an attempt to obtain information was the violation; Justice Alito, concurring, argued that the *monitoring* was a violation of Jones's reasonable expectation of privacy; and Justice Sotomayor, also concurring, agreed with them both, but would provide further Fourth Amendment protections. This report will examine these three decisions in an effort to find their place in the body of existing Fourth Amendment law pertaining to privacy, property, and technology.

In *Jones*, the police attached a GPS tracking device to the bottom of Jones's car and monitored his movements for 28 days. At trial, the prosecution relied on Jones's movements to a stash house to tie him to a drug conspiracy. Jones was convicted and given a life sentence. The United States Court of Appeals for the District of Columbia Circuit reversed, holding that the evidence was unlawfully obtained under the Fourth Amendment. The Supreme Court agreed. The majority, speaking through Justice Scalia, explained that a physical intrusion into a constitutionally protected area, coupled with an attempt to obtain information, can constitute a violation of the Fourth Amendment. Although the Court's landmark decision in *Katz v. United States*, 389 U.S. 347 (1967), supposedly altered the focus of the Fourth Amendment from property to privacy, the majority argued that it left untouched traditional spheres of Fourth Amendment protection—a person and his house, papers, and effects. Because the police had invaded Jones's property—his car, which is an *effect*—that was all the Court needed to hold that a constitutional search had occurred.

The majority's test, however, provides little guidance in instances where the government need not physically install a device to conduct surveillance, for instance, by using cell phones or preinstalled GPS devices in vehicles.

To understand how the Court may rule on these technologies, one must look to the two concurrences, which provide a more global interpretation of the Fourth Amendment. Justice Alito, writing for a four-member concurrence, would have applied the *Katz* privacy formulation, asserting that longer-term monitoring constitutes an invasion of privacy, whereas short-term monitoring does not. He left it to future courts to distinguish between the two.

Justice Sotomayor's concurrence appears to provide the most protection, finding that both the trespass approach and the privacy-based approach should be utilized. She also questioned

the rule that any information provided to a third party, which occurs in many commercial transactions like banking or computing, should lose all privacy protections.

Although all three opinions concluded that the government's action in *Jones* was a search, none expressly required that police get a warrant in future GPS tracking cases. (The government forfeited the argument.) Further, there is no clear indication of the level of suspicion—probable cause, reasonable suspicion, or something less—that is required to attach a GPS unit and monitor the target's movements. Additionally, there have been several bills filed in the 112th Congress, including Senator Patrick J. Leahy's Electronic Communications Privacy Act Amendment Act of 2011 (S. 1011) and Senator Ron Wyden's and Representative Jason Chaffetz's identical legislation, S. 1212 and H.R. 2168, the Geolocational Privacy and Surveillance Act (GPS bill), that would require a warrant based upon probable cause to access geolocation information.

Chapter 4 – Congress enacted the USA PATRIOT Act soon after the 9/11 terrorist attacks. The most controversial sections of the act facilitate the federal government's collection of more information, from a greater number of sources, than had previously been authorized in criminal or foreign intelligence investigations. The Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA), and the national security letter (NSL) statutes were all bolstered. With the changes came greater access to records showing an individual's spending and communication patterns as well as increased authority to intercept e-mail and telephone conversations and to search homes and businesses. In some cases, evidentiary standards required to obtain court approval for the collection of information were lowered. Other approaches included expanding the scope of information subject to search, adding flexibility to the methods by which information could be collected, and broadening the purposes for which information may be sought.

Some perceived the changes as necessary to unearth terrorist cells and update investigative authorities to respond to the new technologies and characteristics of ever-shifting threats. Others argued that authorities granted by the USA PATRIOT Act and subsequent measures could unnecessarily undermine constitutional rights over time. In response to such concerns, sunset provisions were established for many of the changes.

Subsequent legislation made most of these changes permanent. However, a number of authorities affecting the collection of foreign intelligence information are still temporary. Three such provisions (the lone wolf, roving wiretap, and business record sections of FISA) are set to expire on June 1, 2015. Additionally, provisions added by the FISA Amendments Act of 2008, relating to the use of foreign intelligence tools to target individuals while they are reasonably believed to be abroad, will expire on December 31, 2012.

Chapter 5 – This report provides an overview of federal law governing wiretapping and electronic eavesdropping under the Electronic Communications Privacy Act (ECPA). It also appends citations to state law in the area and the text of ECPA.

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given his prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than five years; fines up to $250,000 (up to $500,000 for organizations); civil liability for damages, attorneys' fees and possibly punitive damages; disciplinary action against any attorneys involved; and suppression of any derivative evidence. Congress has created separate, but comparable,

protective schemes for electronic communications (e.g., email) and against the surreptitious use of telephone call monitoring practices such as pen registers and trap and trace devices.

Each of these protective schemes comes with a procedural mechanism to afford limited law enforcement access to private communications and communications records under conditions consistent with the dictates of the Fourth Amendment. The government has been given narrowly confined authority to engage in electronic surveillance, conduct physical searches, and install and use pen registers and trap and trace devices for law enforcement purposes under ECPA and for purposes of foreign intelligence gathering under the Foreign Intelligence Surveillance Act.

CONTENTS

In: Privacy: Select Issues and Laws for the 21st Century ISBN: 978-1-62618-429-9
Editor: Doris B. Delrio

Chapter 1

SMART METER DATA: PRIVACY AND CYBERSECURITY*

Brandon J. Murrill, Edward C. Liu and Richard M. Thompson

SUMMARY

Fueled by stimulus funding in the American Recovery and Reinvestment Act of 2009 (ARRA), electric utilities have accelerated their deployment of smart meters to millions of homes across the United States with help from the Department of Energy's Smart Grid Investment Grant program.

As the meters multiply, so do issues concerning the privacy and security of the data collected by the new technology. This Advanced Metering Infrastructure (AMI) promises to increase energy efficiency, bolster electric power grid reliability, and facilitate demand response, among other benefits. However, to fulfill these ends, smart meters must record near-real time data on consumer electricity usage and transmit the data to utilities over great distances via communications networks that serve the smart grid. Detailed electricity usage data offers a window into the lives of people inside of a home by revealing what individual appliances they are using, and the transmission of the data potentially subjects this information to interception or theft by unauthorized third parties or hackers.

Unforeseen consequences under federal law may result from the installation of smart meters and the communications technologies that accompany them. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It begins with an examination of the constitutional provisions in the Fourth Amendment that may apply to the data. As we progress into the 21st century, access to personal data, including information generated from smart meters, is a new frontier for police investigations. The Fourth Amendment generally requires police to have probable cause to search an area in which a person has a reasonable expectation of privacy.

---

* This is an edited, reformatted and augmented version of a Congressional Research Service publication, CRS Report for Congress R42338, from www.crs.gov, prepared for Members and Committees of Congress, dated February 3, 2012.

However, courts have used the third-party doctrine to deny protection to information a customer gives to a business as part of their commercial relationship. This rule is used by police to access bank records, telephone records, and traditional utility records. Nevertheless, there are several core differences between smart meters and the general third-party cases that may cause concerns about its application. These include concerns expressed by the courts and Congress about the ability of technology to potentially erode individuals' privacy.

If smart meter data and transmissions fall outside of the protection of the Fourth Amendment, they may still be protected from unauthorized disclosure or access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). These statutes, however, would appear to permit law enforcement to access smart meter data for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA), subject to certain conditions. Additionally, an electric utility's privacy and security practices with regard to consumer data may be subject to Section 5 of the Federal Trade Commission Act (FTC Act). The Federal Trade Commission (FTC) has recently focused its consumer protection enforcement on entities that violate their privacy policies or fail to protect data from unauthorized access. This authority could apply to electric utilities in possession of smart meter data, provided that the FTC has statutory jurisdiction over them. General federal privacy safeguards provided under the Federal Privacy Act of 1974 (FPA) protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities.

OVERVIEW

Smart meter technology is a key component of the Advanced Metering Infrastructure (AMI)[1] that will help the smart grid [2] link the "two-way flow of electricity with the two-way flow of information."[3] Privacy and security concerns surrounding smart meter technology arise from the meters' essential functions, which include (1) recording near-real time data on consumer electricity usage; (2) transmitting this data to the smart grid using a variety of communications technologies;[4] and (3) receiving communications from the smart grid, such as real-time energy prices or remote commands that can alter a consumer's electricity usage to facilitate demand response.[5]

Beneficial uses of AMI are developing rapidly, and like the early Internet, many applications remain unforeseen.[6] At a basic level, smart meters will permit utilities to "collect, measure, and analyze energy consumption data for grid management, outage notification, and billing purposes."[7] The meters may increase energy efficiency by giving consumers greater control over their use of electricity,[8] as well as permitting better integration of plug-in electric vehicles and renewable energy sources.[9] They may also aid in the development of a more reliable electricity grid that is better equipped to withstand cyber attacks and natural disasters, and help to decrease peak demand for electricity.[10] To be useful for these purposes, and many others, data recorded by smart meters must be highly detailed, and, consequently, it may show what individual appliances a consumer is using.[11] The data must also be transmitted to electric utilities—and possibly to third parties outside of the smart grid—subjecting it to potential interception or theft as it travels over communications networks and is stored in a variety of physical locations.[12]

These characteristics of smart meter data present privacy and security concerns that are likely to become more prevalent as government-backed initiatives expand deployment of the meters to millions of homes across the country. In the American Recovery and Reinvestment Act of 2009 (ARRA), Congress appropriated funds for the implementation of the Smart Grid Investment Grant (SGIG) program administered by the Department of Energy.[13] This program now permits the federal government to reimburse up to 50% of eligible smart grid investments, which include the cost to electric utilities of buying and installing smart meters.[14] In its annual report on smart meter deployment, the Federal Energy Regulatory Commission cited statistics showing that the SGIG program has helped fund the deployment of about 7.2 million meters as of September 2011.[15] At completion, the program will have partially funded the installation of 15.5 million meters.[16] By 2015, the Institute for Electric Efficiency expects that a total of 65 million smart meters will be in operation throughout the United States.[17]

Installation of smart meters and the communications technologies that accompany them may have unforeseen legal consequences for those who generate, seek, or use the data recorded by the meters. These consequences may arise under existing federal laws or constitutional provisions governing the privacy of electronic communications, data retention, computer misuse, foreign surveillance, and consumer protection. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It examines the legal implications of smart meter technology for consumers who generate the data, law enforcement officers who seek smart meter data from utilities, utilities that store the data, and hackers who access smart grid technology to steal consumer data or interfere with it. This report looks at federal laws that may pertain to the data when it is (1) stored in a utility-owned smart meter at a consumer's residence; (2) in transit between the meter and the smart grid by way of various communications technologies; and (3) stored on computers in the grid. This report does not address state or local laws, such as regulations by state Public Utilities Commissions, that may establish additional responsibilities for some electric utilities with regard to smart meter data. It also does not discuss the mandatory cybersecurity and reliability standards enforced by the North American Electric Reliability Corporation, which impose obligations on utilities that participate in the generation or transmission of electricity.[18]

General federal privacy safeguards provided under the Federal Privacy Act of 1974 (FPA) protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities. Section 5 of the Federal Trade Commission Act (FTC Act) allows the Federal Trade Commission (FTC) to bring enforcement proceedings against electric utilities that violate their privacy policies or fail to protect meter data from unauthorized access, provided that the FTC has statutory jurisdiction over the utilities.

It is unclear how Fourth Amendment protection from unreasonable search and seizures would apply to smart meter data, due to the lack of cases on this issue. However, depending upon the manner in which smart meter services are presented to consumers, smart meter data may be protected from unauthorized disclosure or unauthorized access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). If smart meter data is protected by these statutes, law enforcement would still appear to have the ability to access it for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA).

SMART METER DATA: PRIVACY AND SECURITY CONCERNS

Residential smart meters present privacy and cybersecurity issues[19] that are likely to evolve with the technology.[20]

In 2010, the National Institute of Standards and Technology (NIST) published a report identifying some of these issues, which fall into two main categories: (1) privacy concerns that smart meters will reveal the activities of people inside of a home by measuring their electricity usage frequently over time;[21] and (2) fears that inadequate cybersecurity measures surrounding the digital transmission of smart meter data will expose it to misuse by authorized and unauthorized users of the data.[22]

Detailed Information on Household Activities

Smart meters offer a significantly more detailed illustration of a consumer's energy usage than regular meters.

Traditional meters display data on a consumer's *total* electricity usage and are typically read manually once per month.[23] In contrast, smart meters can provide *near real-time* usage data by measuring usage electronically at a much greater frequency, such as once every 15 minutes.[24] Current smart meter technology allows utilities to measure usage as frequently as once every minute.[25]

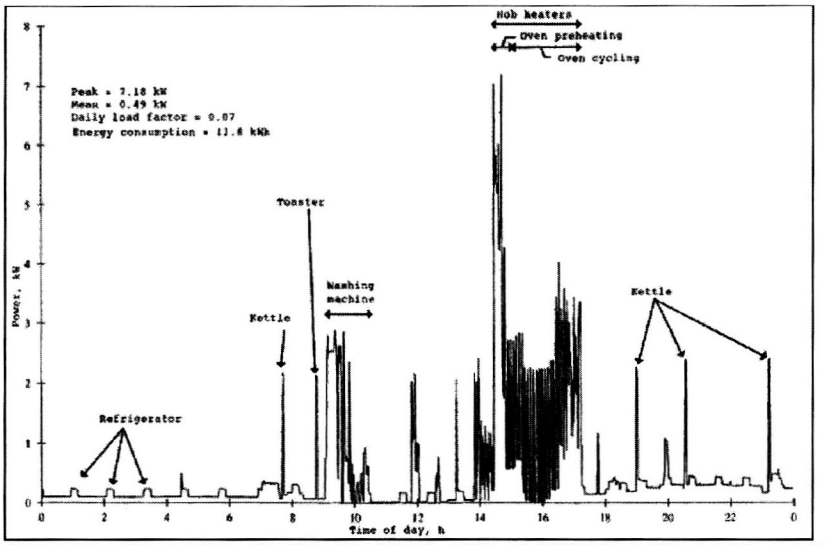
By examining smart meter data, it is possible to identify which appliances a consumer is using and at what times of the day, because each type of appliance generates a unique electric load "signature."[26]

NIST wrote in 2010 that "research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances."[27]

A report for the Colorado Public Utilities Commission discussed an Italian study that used "artificial neural networks" to identify individual "heavy-load appliance uses" with 90% accuracy using 15-minute interval data from a smart meter.[28] Similarly, software-based algorithms would likely allow a person to extract the unique signatures of individual appliances from meter data that has been collected less frequently and is therefore less detailed.[29]

By combining appliance usage patterns, an observer could discern the behavior of occupants in a home over a period of time.[30] For example, the data could show whether a residence is occupied, how many people live in it, and whether it is "occupied by more people than usual."[31]

According to the Department of Energy, smart meters may be able to reveal occupants' "daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment."[32] *Figure 1*, which appears in NIST's report on smart grid cybersecurity, shows how smart meter data could be used to decipher the activities of a home's occupants by matching data on their electricity usage with known appliance load signatures.



Source: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 13 (2010), available at http://csrc.nist.gov/ publications /nistir /ir7628/ nistir-7628_vol2.pdf.

Note: Researchers constructed this picture from electricity usage data collected at one-minute intervals using a nonintrusive appliance load monitoring (NALM) device, which is similar to a smart meter in the way that it records usage data. For a comparison of the technologies, see COLORADO PRIVACY REPORT, supra note 6, at A-1 to A-9.

Figure 1. Identification of Household Activities from Electricity Usage Data. Unique Electric Load Signatures of Common Household Appliances.

Smart meter data that reveals which appliances a consumer is using has potential value for third parties, including the government. In the past, law enforcement agents have examined *monthly* electricity usage data from *traditional* meters in investigations of people they suspected of illegally growing marijuana.[33] For example, in *United States v. Kyllo*, a federal agent subpoenaed the suspect's electricity usage records from the utility and "compared the records to a spreadsheet for estimating average electrical use and concluded that Kyllo's electrical usage was abnormally high, indicating a possible indoor marijuana grow operation."[34] If law enforcement officers obtained near-real time data on a consumer's electricity usage from the utility company, their ability to monitor household activities would be amplified significantly.[35] For example, by observing when occupants use the most electricity, it may be possible to discern their daily schedules.[36]

As smart meter technology develops and usage data grows more detailed, it could also become more valuable to private third parties outside of the grid.[37] Data that reveals which appliances a person is using could permit health insurance companies to determine whether a household uses certain medical devices, and appliance manufacturers to establish whether a warranty has been violated.[38] Marketers could use it to make targeted advertisements.[39] Criminals could use it to time a burglary and figure out which appliances they would like to steal.[40] If a consumer owned a plug-in electric vehicle, data about where the vehicle has been charged could permit someone to identify a person's location and travel history.[41]

Even privacy safeguards, such as "anonymizing" data so that it does not reflect identity, are not foolproof.[42] By comparing anonymous data with information available in the public

domain, it is sometimes possible to identify an individual—or, in the context of smart meter data, a particular household.[43] Moreover, a smart grid will collect more than just electricity usage data. It will also store data on the account holder's name, service address, billing information, networked appliances in the home, and meter IP address, among other information.[44] Many smart meters will also provide transactional records as they send data to the grid, which would show the time that the meter transmitted the data and the location or identity of the transmitter.[45]

Increased Potential for Theft or Breach of Data

Smart grid technology relies heavily on two-way communication to increase energy efficiency and reliability, including communication between smart meters and the utility (or other entity) that stores data for the grid.[46] Many different technologies will transmit data to the grid, including "traditional twisted-copper phone lines, cable lines, fiber optic cable, cellular, satellite, microwave, WiMAX, power line carrier, and broadband over power line."[47] Of these communications platforms, wireless technologies are likely to play a "prominent role" because they present fewer safety concerns and cost less to implement than wireline technologies.[48] According to the Department of Energy, a typical utility network has four "tiers" that collect and transmit data from the consumer to the utility.[49] These include "(1) the core backbone—the primary path to the utility data center; (2) backhaul distribution—the aggregation point for neighborhood data; (3) the access point—typically the smart meter; and, (4) the HAN—the home network."[50] Energy usage data moves from the smart meter,[51] and then to an "aggregation point" outside of the residence such as "a substation, a utility pole-mounted device, or a communications tower."[52] The aggregation points gather data from multiple meters and "backhaul" it to the utility using fiber, T1, microwave, or wireless technology.[53] Utilities typically rely on their own private networks to communicate with smart meters because they have found these networks to be more reliable and less expensive than commercial networks.[54]

As NIST explains, consumer data moving through a smart grid becomes stored in many locations both within the grid and within the physical world.[55] Thus, because it is widely dispersed, it becomes more vulnerable to interception by unauthorized parties[56] and to accidental breach.[57] The movement of data also increases the potential for it to be stolen by unauthorized third parties while it is in transit, particularly when it travels over a wireless network[58]—or through communications components that may be incompatible with one another or possess outdated security protections.[59]

Smart Meters and the Fourth Amendment

The use of smart meters presents the recurring conflict between law enforcement's need to effectively investigate and combat crime and our desire for privacy while in our homes. With smart meters, police will have access to data that might be used to track residents' daily lives and routines while in their homes, including their eating, sleeping, and showering habits, what appliances they use and when, and whether they prefer the television to the treadmill,