CONTRIBUTED PAPER

Privacy-Aware Design Principles for Information Networks

In this paper, the authors introduce five privacy-aware principles that should enable designers to create mobile networks that address the anxieties of individual users and the public at large by minimizing the collection of personal data.

By Stephen B. Wicker, *Fellow IEEE* and Dawn E. Schrader

ABSTRACT | Privacy has become a critical topic in the engineering of networked systems. Electronic surveillance, both covert and overt, has a negative impact on both the individual and society, and the public's perception of engineered systems that forsake the privacy issue is increasingly negative. Engineers and computer scientists thus have a moral obligation to avoid design choices that are unnecessarily privacy invasive. To fully illustrate this point, we provide an overview of the philosophical, legal, moral, and epistemological literature on the subject of privacy and related implications of its invasion. We then introduce a series of privacy-aware design principles that lead to less invasive information technologies. We develop a smart grid/demand response case study to illustrate the impact of the proposed design rules that protect individual privacy and promote understanding of ethical issues underlying the need for privacy for individuals and society.

KEYWORDS | Communication networks; computer networks; ethical aspects; privacy; technology social factors

I. INTRODUCTION

Information networks collect and convey data about individual behavior and preferences. Networks of video cameras, for example, are often used to monitor behavior on urban streets. In such cases, there is a clear and public connection between the collected data (e.g., video of a street corner at night) and the public mission of the system (e.g., crime deterrence). Such surveillance may be problematic, but the connection between the collection of the data and the mission of the system is both clear and public. In other cases, however, data collection systems serve as supporting, and in some cases hidden, architectural components of larger systems. Examples can be found in mobile communication and computing networks as well as infrastructure monitoring and control systems. Take for example the collection of location data in cellular systems. Location data are used in cellular systems for the routing of incoming calls, to facilitate handoffs, and to speed the response of emergency services. Location data are clearly functionally useful, but as we will see, substantial economic, legal, and social consequences have arisen from the collection and storage of this type of data. Finally, data collection may simply be an inadvertent and unnecessary result of a bad design. Google, for example, may face legal sanctions for accidentally collecting "snippets of unencrypted Internet information . . . including passwords and the contents of some e-mails" while mapping the location of WiFi routers around the world [1].

The incorporation of data collection elements in networked systems results from design choices, choices that have implications for the privacy of those that use or somehow come into contact with the system. We argue that such design choices have both technical and moral implications, and can have serious downstream societal consequences. Engineers and computer scientists often argue that any moral issues that arise from the creation of a technological artifact are a function of the use of that artifact, and not the design of the artifact itself.[1] In essence, the argument is that design choices are morally neutral; it is only in action with or upon artifacts that moral issues

Manuscript received May 4, 2010; accepted July 7, 2010. Date of publication October 28, 2010; date of current version January 19, 2011. This work was supported in part by the National Science Foundation TRUST Science and Technology Center and the National Science Foundation Trustworhty Computing Program.
S. B. Wicker is with the Department of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14853 USA (e-mail: wicker@ece.cornell.edu).
D. E. Schrader is with the Department of Education, Cornell University, Ithaca, NY 14853 USA (e-mail: dawn.schrader@cornell.edu).
Digital Object Identifier: 10.1109/JPROC.2010.2073670

[1]See Clarke, "Information technology and dataveillance," *Commun. ACM*, Vol. 31, No. 5, May 1988, p. 510: "It would be inappropriate for the purveyors of any technology to be responsible for decisions regarding its application. The technologist has an unavoidable interest in the outcome, and cannot appreciate and take into consideration the interests of the many different social groups who may consider themselves to be affected."

enter our concerns. When one considers poorly designed automobiles and dangerous children's toys, such a stance is clearly tenuous. This is also a tenuous position when one considers the design of cellular networks and other technologies; however unintentionally, such systems have become a prominent source of privacy invasion. Privacy and its invasion is a moral issue in which the individual's autonomy and right to self-determination is fundamentally at risk. It follows that a moral perspective must be integrated into information network design practices; a perspective that calls for privacy awareness in *both* design and use.

In this paper, we investigate the technical, legal, and moral issues that arise from the incorporation of data collection into networked computing and communication systems. We then propose a set of privacy-aware design principles—a design methodology that highlights privacy concerns and guides the practicing engineer or computer scientist in the creation of mobile computing and communication networks that minimize the potential for the invasion of the privacy of individual users and the public at large. The proposed design principles are derived from the Fair Information Practices developed by the Department of Health, Education, and Welfare (HEW) in the 1970s [2]. At the core of the proposed principles lie requirements that the collection of personally identifying information be minimized. We propose that such collection should be a functional requirement of the system, and that when collected, data be used only locally wherever possible. The latter results in a distributed processing requirement that drives the selection of architectures for a wide variety of information networking systems.

Privacy-aware design often calls for creativity and the solution of a series of interesting technical problems. For example, if one accepts the proposition that frequency reuse is critical to mobile telephony, and that the resulting cellular architecture requires the collection of location data for the routing of incoming calls, one is left with the conundrum of how to avoid collecting location data from cellular users. We will show that privacy-aware design points to anonymous user authentication as a potential solution to the privacy invasion problem.

The need for fine-grained power consumption data in demand response systems creates another privacy problem; as we demonstrated in other work [44], such data reveals detailed behavior within the home. In this example, privacy-aware design points to both distributed processing and anonymization through aggregation. In this paper, we will explore both anonymous user authentication and privacy-aware demand response as case studies for the principles developed.

What follows is a brief overview of the philosophical and legal privacy literature. We emphasize the impact of privacy invasion, and assert that in many cases invasion derives from inadvertent design choices. We then introduce our privacy-aware design principles, and highlight the technical and moral problems that emerge from the application of these principles. We then demonstrate, through the case studies, how privacy-aware design principles can be applied.

II. THE NATURE OF PRIVACY AND ITS INVASION

Privacy has proven to be an extremely difficult concept to define. There is an extensive literature consisting of proposed definitions and subsequent critiques of those definitions (see, for example, [3]). Part of the definitional problem lies in the breadth of the topic; privacy law, for example, covers issues as diverse as freedom of speech, freedom of religion, search and seizure, and marital rights. For the purposes of this paper, however, our goal is to develop a working set of concepts with which we can identify potential invasions of privacy that may occur through choices made in the design of information technology. The result will be the notion of a context-based zone of seclusion, with which we can evaluate the privacy impact of candidate technologies.

A. Defining Privacy

One of the earliest attempts to connect privacy and the potential danger of new technologies lies in an 1890 *Harvard Law Review* article[2] by Warren and Brandeis entitled "The right to privacy" [4]. In this article, Warren and Brandeis identified a preexisting basis for privacy torts[3] in various common law[4] precedents. Their basic thesis was that monetary damages and, in some cases, an injunction are appropriate when information about or a representation of an individual is published without the individual's consent.

Warren and Brandeis' working definition for the right to privacy was the right "to be let alone"—a phrase taken from an earlier work by Judge Thomas Cooley [5]. Warren and Brandeis claimed that there was a growing threat to this right, pointing to "recent inventions and business methods" as the cause. As seen in the following excerpt, particular emphasis was placed on "instantaneous

[2]"The right to privacy" is often referred to as one of the most frequently cited law review articles ever written, and is an "unquestioned classic." See Shapiro, "The most-cited law review articles" *California Law Rev.* 73.5 (1985), pp. 1540–1554. Available at: http://works.bepress.com/aallcallforpapers/59.

[3]"A tort is an act that injures someone in some way, and for which the injured person may sue the wrongdoer for damages. Legally, torts are called civil wrongs, as opposed to criminal ones." See http://www.lectlaw.com/def2/t032.htm.

[4]Common law is based on the decisions of courts. It is often contrasted with civil law, which is based on legislative statutes or executive branch action. The legal system of the United Kingdom (and derivatively, that of the United States, with the notable exception of Louisiana) is based on common law, while that of France and most other European countries is based on civil law. For a more detailed discussion, see van Caenegem, *The Birth of the English Common Law*, 2nd Ed., Cambridge, U.K.: Cambridge Univ. Press, 1988, or Cantor, *Imagining the Law: Common Law and the Foundations of the American Legal System*, New York: Perennial, 1999.

photographs" and the newspapers that were anxious to publish them.

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops" [4].

The "instantaneous photographs" referred to here were the products of the first handheld cameras; they should not be confused with the Polaroid instant-film cameras developed almost 80 years later. Handheld cameras created a new privacy problem in that they allowed for the photography of unwilling, or even unknowing persons.

Warren and Brandeis spoke of the right to be let alone as a general right that includes the right to prevent publication of one's "thoughts, sentiments, and emotions." Warren and Brandeis suggested that one's thoughts, sentiments, and emotions could be viewed as one's private property and might fall under the protection of well-recognized property rights. But they felt it would be more appropriate to consider the underlying principle on which the right to privacy rests to be that "of an inviolate personality."

Warren and Brandeis thus connected an individual's ability to maintain control over the revelation of personal information to the presence of a space for individual development in which one is safe from outside interference. As we show in a later section, the threats of both overt and covert surveillance to self-development are substantial. It is interesting to note that potential harm to individual autonomy was cited in this seminal article at a time when modern psychology was still in its relative infancy.[5]

In summary, Warren and Brandeis conceived of the right of privacy as the right to be let alone, with the emphasis being placed on the individual's ability to prevent the publication of personal information in a public forum. For our purposes, Warren and Brandeis' conception can be generalized through the metaphor of a zone of seclusion, a zone in which the agent controls access to various types of personal information.[6] The value of such a zone lies in part in the agent's perception of solitude and safety. The agent feels free to exercise various thoughts and behaviors without threat of censure, and is thus able to experiment, finding his or her own way to a sense of self-realization and exercising his or her moral right to autonomy.

Nissenbaum extends and refines the notion of a zone of seclusion through her development of "contextual integrity." As described below, the zone varies depending on context:

> Specifically, whether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination. The model is prescriptive in that it is intended to serve as a justificatory framework for prescribing specific restrictions [6, p. 155].

Privacy may thus be viewed as a zone of seclusion, contextually defined, in which the individual can control access to various types of personal information. In this zone, the individual is free to experiment, develop relationships, and create an autonomous self without fear of censure or manipulation. We will now consider what happens when this zone is invaded. We provide a sampling from this extensive literature, focusing on the moral and epistemic impact of privacy invasion.

B. The Moral Impact of Privacy Invasion

Morality is a system or code of judgment and conduct, and moral choices are decisions individuals make, as autonomous agents, to determine what is right and good as they live their lives in interaction with others. Surveillance and the collection of personal information become moral issues when the information collection is used to interfere with individual autonomy and decision making.

As noted above, Nissenbaum approaches the impact of privacy invasion through the lens of contextual integrity. She argues that when social privacy norms are violated or threatened in particular contexts, there is a threat to fundamental moral values [6]. These values include: 1) prevention of information-based harm, 2) maintenance of informational equality, 3) autonomy, 4) freedom, 5) preservation of important human relationships, and 6) democracy.[7] Advertising is a classic example of an attempt to alter an individual's decision making in accord with external goals separate from that of the individual. The extent to which it becomes a moral issue depends on types of infringement and the specific case and/or context.

The potential infringement of moral values by information technologies is particularly apparent with Nissenbaum's first two values, as user data collected by Internet and cell phone service providers, for example, allow for manipulative advertising while creating the

[5]James' *Principles of Psychology* was published in 1890—the same year as the Warren/Brandeis article. At this same time, Freud was conducting the initial research that would lead to the publication of *The Interpretation of Dreams* in 1900.

[6]See [54, ch. 4–6].

[7]Nissenbaum cites Cohen, Benn, Gavison, van den Hoven, Nehf, Schwartz, Reiman, and Rosen, among others, who also concur with this list of values [6, p. 146].

Kafkaesque sense of information imbalance familiar to anyone who has ever tried to call a utility or service provider, or has taken a call from a telemarketer. Though in a less obvious manner, privacy invasion by information technologies may pose threats to the other values as well.

Along similar lines, Cohen claims that the moral impact of privacy invasion extends beyond simple ethical behavior and choice to the very nature of the self and one's autonomy as an ethical agent. She has written that "data privacy protection furthers still another sort of liberty—that of self-determination, expressed through the power to define oneself to the world in the way one wishes" [7].

Surveillance thus limits the moral agency of individuals by infringing on their right to privacy, which in turn limits freedom of self-definition, judgment, choice, and action. Note that some of these values have clear connections to societal institutions. Democratic institutions, for example, rely on individuals to make well-considered decisions about societal boundaries, governmental processes, and the selection of leaders. For example, in *The Myth of Digital Democracy*, Hindman addresses the potential threat to democratic systems posed by the structure of and information collection on the World Wide Web [8].

On the specific issue of marketing, Gandy argues that marketers use personal information to discriminate; to sort individuals into classes of those more likely or less likely to purchase a given product. Individuals are thus relegated to different information streams, with some being offered choices that others never see. Marketers thus circumscribe individual decision-making by limiting available choices [9]. Whether this is a moral issue depends upon what information is limited, and to whom. There is potential for ethnic, racial, socioeconomic, and other forms of discrimination when options such as access to information, health care or educational opportunities, for example, are limited by one's previous choices and behaviors as reflected in data collected and recycled for marketing purposes.

Moral issues also arise in contexts in which the individual is asked to give up his or her privacy in return for being allowed to use a given information technology. Even if people freely give up their privacy for the sake of expedience, or for utilitarian benefit of the greater good, they are still giving up a fundamental moral right, and a problem arises when they do not fully understand the consequences of this surrender [10]. An extensive literature has developed over the exemplary case of adolescents who are apparently quite willing to give up their privacy on social networking sites, and the potential impact of that surrender [11]. A frequently cited answer is that the adolescents are not aware of what they are giving up, the moral implications of giving up privacy, or more pragmatically, how giving away private information may affect their future in terms of employment opportunities, access to education, goods and services, and the like.

The question here is far larger—why are Internet, cellular, and other technology users of all ages willing to give up their privacy in return for the expediency of using the given technology? It may be that most users are unaware of the extent of their exposure, and it is also the case that they have little choice. In our modern context, it is simply too difficult to conduct one's life and interact with others without using these technologies. The moral choice of maintaining a zone of privacy in the contexts of the use of these technologies has simply been taken away. The fault, in part, lies in the design of these technologies. Technology often requires individuals to freely give up their moral freedom of choice. Another fault lies in the development, or lack thereof, of individuals' critical awareness of their responsibility and role in decision making and choices about their own consumer behavior and their lives. With that comes the corollary lack of development of knowledge as to how to make their own sound, reasoned judgments in the face of conflicting information or disparate points of view. Making such judgments and decisions, we argue, is both a moral and epistemic freedom that unreflective technical development may usurp.

C. The Epistemic Impact of Privacy Invasion

Epistemology is the study of the nature of knowledge and justified belief, focusing on the individual's ability to collect, assess, and integrate knowledge into a coherent worldview. Several social scientists have concluded that privacy invasion puts individuals' epistemic freedom at risk by placing limits on their freedom to think, to challenge, to experiment, and to make well-considered choices. In a society where individual choices are monitored, regulated, and reintroduced to the individual in reduced or abridged form, epistemic as well as moral freedom of thought and action are constrained.

The late French philosopher Foucault provided two perspectives on surveillance and constraints on thought. The first considers surveillance as a permanent and oppressive presence of power that induces passivity in the surveilled. The second perspective, similar to that of Gandy, lies in the use of personal information to place a direct limitation on choice and experimentation.

The oppressive nature of surveillance is often explained through analogy to Bentham's Panopticon [12]. The Panopticon was a proposed prison in which the cells were arranged radially about a central tower. The cells were backlit so that guards in the tower could see the prisoners whenever the guards wished, but the prisoners could never see the guards, and thus never knew whether they were being watched. Bentham characterized the Panopticon as providing a "new mode of obtaining power of mind over mind, in a quantity hitherto without example."

In *Discipline and Punish* [13], Foucault characterized the impact of the Panopticon's as "induc[ing] in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power." Foucault argued that this surveillance and self-consciousness led to an internalization

of discipline that resulted in "docile bodies," bodies that were ideal for the regimented classrooms, factories, and military of the modern age. Such implications seem to appear with current technology, especially among the young, who, without thought (thoughtlessly), comply with computer-driven personal data collection.

With regard to limiting choice, Foucault argued that marketers limit thinking by only offering to the individual that in which the individual has already expressed interest [14]. The result is a constriction of thought and a motivation to follow the path of least resistance. The individual thus delegates epistemic authority to external actors instead of internal resources. The individual is thus trained to limit the extent to which he or she seeks new or disparate information, inhibiting self-determination and reflective judgment, as well as his or her "epistemological power."

Foucault specifically addresses "epistemological power," meaning the power taken by those in control to observe people and use the people's own actions to exercise power over them. Foucault's remarks on the self, and his insight into power, observation, and epistemic exploitation, highlight the need for the maintenance of privacy as paramount to autonomous personhood. He demonstrates that one can be self-consciously aware of one's identity even when immersed in the skewed power relationships inherent in modern social life. That is, that since the information was derived from the self's own actions, and since the individual is aware of being watched, a self-conscious awareness dominates one's own thoughts and therefore guides one's behavior in a self-aware manner. However, this kind of self-awareness is not the general psychological "rule," but is rather the exception. In the face of external pressures, such a high level reflective judgment, as King and Kitchener might describe it, is something that may not be psychologically accessible to all people [15]. To develop such an epistemic perspective requires experience in continually considering and dealing with complex ill-structured problems and opportunities. Providing people with opportunities to make their own choices and decisions about what to do, for example, with regard to their own personal information, and to make judgments in the context of a plethora of possible considerations and options, some even conflicting, may promote such development. To return to our advertising example, if you are limited in the choices due to selective filtering of information, you may not develop the skills necessary to select and cogently justify a purchase of one product over another, since what was offered to you were similar instead of competing products. This is a simple, and nonmoral example, but implications for such products as health care, nutritious and healthy food, housing and schooling options, etc., do indeed have personal and societal moral implications that are grounded in such protracted epistemic development.

Foucault, in his analysis of the influences of power and culture on self, thought, and action, illustrates the power of external forces and the fundamental need of persons to a sense of privacy in order to maintain their own separate sense of self, which is the hallmark of moral autonomy:

> As soon as you start writing, even if it is under your real name, you start to function as somebody slightly different, as a "writer." You establish from yourself to yourself continuities and a level of coherence, which is not quite the same as your real life... All this ends up constituting a kind of neoidentity, which is not identical to your identity as a citizen or your social identity. Besides you know this very well, since you want to protect your private life [16].

This brief review of the extensive literature on the impact of privacy invasion highlights the moral and personal harm to individuals caused by design choices that lead to increased surveillance of individuals. Given the potential for harm, it follows that there is a moral obligation on the part of engineers to pursue privacy-aware designs for mobile computing and communication systems. It is also essential that the general public, the consumers of this technology, understand the mechanisms involved as well as the psychological implications of the collection of personally identifying information. The dissemination of personal information affects individual autonomy and action, and personal control over this information is critical to the maintenance of basic human freedom and dignity.

III. THE MARKET FOR PERSONAL INFORMATION

To fully appreciate the importance of privacy-aware design, one must appreciate the intensity of the desire of markets and government agencies to acquire personally identifying information. To be blunt, any database created by an information network will be commodified in a ready and lucrative market. In this section, we briefly focus on the civilian information marketplace, while acknowledging that there are state and federal issues to be considered as well.[8]

Direct marketing is an enormous industry. According to the Direct Marketing Association, $149.3 billion was spent on direct marketing in 2009—more than half of all advertising expenditures in the United States—with a return of close to $1.783 trillion dollars in sales attributable to the advertising.[9] The latter amounted to 8.3% of total U.S. gross domestic product.

What makes direct marketing direct, of course, is that a given marketing campaign is delivered only to a select subset of consumers. The rationale for increased efficiency

[8]It should be noted that the federal government in particular has been an active consumer in the information marketplace (see [18]).

[9]See http://www.the-dma.org/aboutdma/whatisthedma.shtml.

is intuitive; direct marketing attempts to limit the cost of advertising by limiting the delivery of the advertising pitch to those who are most likely to buy the product. The Direct Marketing Association estimates that each dollar spent on direct marketing provides a return of $11.73, while each dollar spent on nondirect marketing only yields $5.23 [17].

Direct marketers are thus engaged in a grand sorting operation, discriminating among individuals for the purpose of increasing the efficiency of their advertising [18]. Gandy [9] refers to this process of discrimination as the Panoptic sort—an allusion to the above referenced Panopticon of Bentham. The analogy to direct marketing lies in the fact that individuals know that they are under observation, but they do not know the content and the extent of the information being collected.

Credit agencies provide one of the most powerful examples of commercial data collection in the United States. There are three main credit reporting agencies: Experian, Equifax, and TransUnion. These bureaus require reciprocity agreements from their clients—in return for credit information from credit bureaus, credit granting entities must provide information regarding balances, available credit, and payment history [9]. A positive feedback loop is thus created—credit agencies collect data and refine their estimates of creditworthiness, thus making their product more valuable, which in turn leads to a greater demand for their services and a subsequent increase in the amount of data collected.

It should be noted that much of the data collected in the United States are "positive" credit data—data regarding bills paid on time, credit card balances, available credit, and so forth. This is to be distinguished from "negative" data such as missed payments and defaults. In Europe and Australia, it is only the latter that can be legally collected [18, pp. 71, 126], while in the United States both positive and negative credit can be collected and used to discriminate without the consent of the individual involved.

One of the principle issues that arise from the collection of personal data is reuse—the use of collected data for purposes other than those for which the data were originally collected. Credit ratings, for example, are often used in assessing risk for medical insurance. E-Z pass data, which indicate the location of a vehicle at specific times and places have been used as the basis for increasing car insurance rates. Insurance companies also benefit from the efforts of ChoicePoint and Acxiom, which compile data from driving records, accident reports, court proceedings and resell them to insurance companies [18, p. 107].

Information collected through the use and operation of networked infrastructure is also reused in creative ways. For example, the Austin city police used power consumption data, provided without warrant by a local utility, as a means for obtaining search warrants for the homes of consumers who were potentially using heat lamps to grow marijuana indoors [19].

There are many other sources of data available for reuse by marketers, including purchase data from grocery stores (in the form of shoppers' card data), click streams from e-commerce sites, and subscription information from periodicals. Third parties collect these data and create lists of consumers with highly specific attributes. In *The Panoptic Sort*, Gandy captures the state of "The list vendors" in 1993 [9, pp. 90–95]. He notes that Donnelly Marketing Information Services claimed to have 90% of all U.S. households in its database, allowing its clients to generate customer profiles based on "demographics, lifestyles, and retail sales expenditures." Donnelly's mailing services supported list creation based on "mail responsiveness, credit worthiness, vehicle information, ClusterPLUS lifestyles, contributors, financial investments, hobbies, occupations, census demographics, and more" [9, p. 90].

Bringing Donnelly up to date, we found that InfoUSA acquired Donnelly Marketing in 1999 for $200 million in cash [20]. In 2010, InfoUSA maintains a list of 210 million consumers[10] that can be sorted according to a wide variety of categories, including "area codes, zip codes, home value/home ownership, housing type, mortgage, personal finance, hobbies and interests, children/grandparents/veterans, ethnicity, religion, and voter information."[11] InfoUSA also offers "unlimited business credit reports" for a free 72-h trial.

When made available through high-speed networking, data such as the above allow for real-time sorting of individuals as they surf the web. A *Wall Street Journal* investigation discovered that Internet sites have begun to use personal information provided by data analysis firms to alter the presentation seen by the web surfer [21]. The type of characterization provided by companies like $[x+1]$ can be highly specific:

> ... $[x+1]$ correctly identified Carrie Isaac as a young Colorado Springs parent who lives on about $50 000 a year, shops at Wal-Mart and rents kids' videos. The company deduced that Paul Boulifard, a Nashville architect, is childless, likes to travel and buys used cars. And $[x+1]$ determined that Thomas Burney, a Colorado building contractor, is a skier with a college degree and looks like he has good credit [21].

According to the *Wall Street Journal*, such information is provided almost instantaneously, allowing companies like Capital One to integrate $[x+1]$'s characterization into a decision process that drives which credit card offers will be displayed when the potential customer visits their web site. The Panoptic Sort is now operating, quite literally, at the speed of light.

[10]http://www.infousa.com/Home/home/190000.

[11]http://leads.infousa.com/Consumer/Geography.aspx?bas_session=S95154809117258&bas_vendor=190000.

In summary, there is an extremely large market for personally identifying information. When a new communication or computing technology collects such information in the course of its operation, the resulting database becomes a lucrative commodity. There is a strong motivation for the reuse of the collected data, a reuse that may result in epistemic and moral harm not only to the individual but to society as well. In Section IV, we will review the extent to which the individual and society are protected by courts and legislatures.

IV. CASE LAW AND LEGISLATION

In this section, we will track two basic trends. First, when a new information technology is introduced, government, law enforcement, and commercial interests will quickly avail themselves of any personal information that is conveyed or collected by that technology. Second, legislatures and the court system move to protect privacy interests that are implicated by the first trend. As we will see, the second trend moves far more slowly than the first.

The earliest examples of the first trend begin with the earliest (large-scale) electrical communication technology, the telegraph. A few dates will make the case. In 1844, Morse and Cornell laid their first telegraph line between Washington and Baltimore [22, p. 174]. In 1855, Cornell and Sibley formed the national telegraph system, which at Cornell's suggestion was later called "Western Union." A few years later, engineers on both sides of the Civil War were actively tapping lines in an effort to intercept military dispatches [23]. Towards the end of the war, a former stockbroker was convicted of conspiring to intercept telegraph traffic regarding stock transactions and selling it to subscribers [24]. There were also cases at this time of newspapermen intercepting each other's dispatches in an effort to scoop each other's stories [23].

Governmental interest in the contents of personal telegraph communication began at least as early as 1876, when investigators, acting on behalf of a congressional committee investigating real estate fraud, seized three-quarters of a ton of telegraph messages from the offices of the Atlantic and Pacific Telegraph Company. A contemporary article in the *New York Times* referred to the "unconstitutional and indecent use" to which the seized telegraphs were being put; congressional staffers sorted and indexed each telegram while searching for evidence of fraud, creating the potential for blackmail and other extracurricular activities[12] [25].

A few months before Congress intruded into the offices of the Atlantic and Pacific Telegraph Company, the telephone entered the world. U.S. Patent Number 174 465 was granted to Bell on March 7, 1876. It covered "[t]he method of, and apparatus for, transmitting vocal or other sounds telegraphically ... by causing electrical undulations, similar in form to the vibrations of the air accompanying the said vocal or other sounds." The rise of the telephone has been well documented [26]. The Bell Telephone Company was organized on July 9, 1877. Four years after its formation, the renamed American Bell Telephone Company had licensed 132 692 telephones, and all but nine of the cities in the United States with populations over 10 000 had at least one telephone exchange. By 1895, New York police were conducting routine wiretaps without the benefit of warrants [27].

The evolution of the cooperation between the New York Telephone Company and the police in these early years is instructive. In testimony taken in 1916, Swayze, the general counsel for the New York Telephone Company, testified that the practice of wiretapping in New York went back to 1895. Furthermore, as seen in the following excerpt, the practice began in an entirely *ad hoc* manner, with the telephone company cooperating with the police on this basis of simple verbal requests:

> The practice of wiretapping or listening-in goes back as far as 1895. Originally it was done in a loose way on verbal request, and no record was made of it ... two years ago I decided that there ought to be some check to prevent its use becoming wild. If the police or any other officers should use the privilege for their private purposes it would do irreparable damage to the company (Testimony of Swayze, General Counsel of the New York Telephone Company [27]).

Recognizing the potential damage to the New York Telephone Company's reputation, Swayze testified that the company began to require that the police provide a written request.

There were clearly some who felt that this process of seizing telegrams or tapping into telephone calls went against the grain of constitutionally protected freedoms. In the above cited 1876 *New York Times* article on telegram seizure, for example, the author vigorously asserted the alleged unconstitutionality of the seizure. The question remained, however, as to just where in the Constitution one could find protection against arbitrary surveillance of information networks by the government, law enforcement, or commercial interests. The logical place to start looking, both then and now, is in the Fourth Amendment to the United States Constitution—the amendment that protects citizens against "unreasonable search and seizure" by the Federal Government.

A. Information Technology and the Fourth Amendment

The Fourth Amendment has its origins in English common law, descending from a series of decisions that created a legal moat of sorts around one's home. The legal

[12]There is an interesting parallel between the actions of this congressional committee and the modern FBI's use of CARNIVORE in searching through e-mail at ISPs.

notion of a person's home as his or her castle dates back to at least 1505, when Chief Justice John Fineux of the Court of King's Bench declared that "the house of a man is for him his castle and his defence" [28]. In 1604, Sir Edward Coke, then Attorney General of England, echoed that statement, ruling that "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose" [29]. These and similar cases established the requirement for some type of prior authorization before an official was allowed to search an individual's home.

With this tradition in mind, the American colonists vigorously disputed the right of British revenue officers to search their homes for contraband. The officers were armed with prior authorization in the form of *writs of assistance*, a legal instrument that dated back to the reign of Charles II, and was intended to counter smuggling and the consequent loss of import taxes. The writs were problematic, however, in that they did not have a time limit, did not specify the objective of the search, did not specify the place to be searched, and generally led to fishing expeditions in the homes of the colonists. In Paxton's case, tried in Boston, MA, in February 1761, a Massachusetts lawyer named James Otis declared the writs to be "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book" [30]. John Adams pointed to outrage over the practice as the inaugural event in the resistance that led to the American Revolutionary War.[13]

Twenty-eight years later, when the initial amendments to the Constitution were compiled, they included an amendment specifically intended to overturn Paxton's case and prohibit general searches. This amendment, the fourth in what we now call the Bill of Rights, reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The requirement that a warrant be issued before "persons, houses, papers, and effects" could be searched and seized is thus almost as old as the Republic, with the underlying tradition dating far earlier. Before such a warrant is issued the person requesting the warrant must demonstrate and affirm probable cause that a crime has been committed, and the warrant must be specific as to the place to be searched and the items or persons to be seized.

[13]As quoted and described by Justice Bradley in Boyd v. United States, 116 U. S. 616 (1886). See also Cuddihy, *The Fourth Amendment: Origins and Original Meaning*, Oxford, U.K.: Oxford Univ. Press, 2009.

The amendment's language says nothing, however, that can be *directly* applied to electronic communication. The means by which legal protection against electronic surveillance evolved through judicial interpretation of the Fourth Amendment is the subject of this section. In what follows, we will distinguish between the content of the communication and its context; as will be shown, the two receive significantly different levels of protection.

1) Content Protection: The Supreme Court did not consider whether the Fourth Amendment applied to the content of telephone calls until 1928. The case Olmstead v. United States involved a Prohibition-era bootlegger named Roy Olmstead [31]. Olmstead's operation was immense; he employed two ships and 50 people, while maintaining an underground storage facility near Seattle, WA. His annual sales exceeded two million dollars a year (in 1928 dollars). The FBI determined the extent of this operation by placing wiretaps, without a warrant, in the basement of Olmstead's office building. Olmstead was subsequently tried and convicted of multiple violations of the Volstead Act. He appealed to the Supreme Court, asserting that his Fourth Amendment rights had been violated—the FBI should have obtained a warrant before placing the wiretaps.

Writing for the majority, Chief Justice Taft adopted a limited interpretation of the Fourth Amendment:

> The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants [31].

Taft's rationale was that listening in on a conversation was not the same as searching through a person's belongings. Furthermore, Taft's opinion held that a wiretap does not seize any tangible property of the targeted individual. Olmstead would remain the law of the land for almost 40 years, when a majority of the Court connected the underlying motivation for the Fourth Amendment to the mechanics of and the potential harm caused by wiretapping.

At least one member of the Court recognized the harm associated with wiretapping back in 1928. Justice Brandeis, coauthor of the aforementioned *Harvard Law Review* article "The right to privacy," was at the time of the Olmstead decision an associate justice on the Court. He characterized the invasion of privacy inherent in wiretapping in eloquent terms:

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper,

> confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping [31].

Note the reference to "tyranny and oppression," where Justice Brandeis anticipated the work of Foucault and others who wrote of the internalization of power effected through surveillance. Again, clearly, the moral and epistemic issues underlie the privacy debate.

Justice Brandeis' opinion would eventually be shared by a majority of the Court, but this would not happen until 1967, when the Olmstead decision was reversed in Katz v. United States [32]. The Supreme Court considered the case of Charles Katz, who had used a pay phone in Los Angeles to place illegal bets in Miami and Boston. Without obtaining a warrant, FBI agents placed listening devices outside of the phone booth and recorded Katz' end of several conversations. The transcripts of these conversations were introduced during Katz' trial, and presumably played a role in his conviction. In response to his appeal, the Supreme Court held that tapping calls placed from a telephone booth required a warrant. The majority opinion explicitly overturned Olmstead, holding that the Fourth Amendment "protects people, not places," and that electronic communication was to receive the same Fourth Amendment protection as personal books and papers.

Justice Harlan's concurring opinion introduced a two-part test for the application of Fourth Amendment protection that remains the standard today:

- the person must have exhibited "an actual (albeit subjective) expectation of privacy";
- this expectation is one that "society is prepared to recognize as 'reasonable'."

Ninety one years after Bell received his first patent, the U.S. Supreme Court began to apply Fourth Amendment protection to the content of telephone calls. Today, it is actually rather difficult to obtain a warrant for a wiretap—wiretaps are only allowed when certain crimes are at issue, they are only allowed for a fixed period of time, and the requestor must show that the information sought through the warrant cannot be obtained through other means.

Over the course of time, however, the test that was established in the Katz case proved to be highly malleable. As we show in the following section on context protection, one result was that the context of telephone and other electronic communication did not receive the same protection as its content.

2) Context Protection: The distinction between the content of electronic communication and its context is best understood in terms of the difference between the content of a written letter and the envelope in which it is mailed. Legal scholar and former prosecutor Kerr summarized the difference as follows [52]:

> The essential distinction between content and envelope information remains constant across different technologies, from postal to e-mail. With postal mail, the content information is the letter itself, stored safely inside its envelope. The envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed.
>
> Similar distinctions exist for telephone conversations. The content information for a telephone call is the actual conversation between participants that can be captured by an audio recording of the call. The envelope information includes the number the caller dials, the number from which the caller dials, the time of the call, and its duration.

The primary key to understanding the Court's treatment of context information is another case involving a bootlegger, Miller v. United States [33]. The Miller case involved a modern-day bootlegger; prohibition was not the issue here, the focus was instead on the more mundane matter of taxation. While putting out a fire at Miller's warehouse, firefighters and police discovered 175 gallons of whiskey that did not have the requisite tax stamps. Investigators obtained, without a warrant, copies of Miller's deposit slips and checks. The canceled checks showed that Miller had purchased material for the construction of a still. Miller was subsequently convicted of possessing an unregistered still. Miller appealed, claiming that his Fourth Amendment rights had been violated—the investigators should have obtained a warrant before acquiring his bank records. The Supreme Court disagreed. Writing for the Court, Justice Powell applied Justice Harlan's two-part test from the Katz case as follows:

> There is no legitimate "expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential communications, but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business [33].

Justice Powell had concluded that information "voluntarily conveyed" and "exposed" in the ordinary course of using an information technology was not protected by the Fourth Amendment. If we consider the use of a cellular telephone—a technology that was in the early stages of its development at the time of the Miller ruling—we might conclude that all of the information transmitted

by that telephone in the course of making it a functioning part of the cellular network—messages supporting registration, call setup, roaming, and handoff—are not protected by the Fourth Amendment.

The content/context distinction played a significant role in the case of Smith v. Maryland [34], one of the first in which the Miller ruling was explicitly applied to electronic communication. In this case, one Michael Lee Smith robbed a woman's home and then made harassing telephone calls to the woman after the fact. In response to a request from investigators, the telephone company installed a *pen register* at the central office that served Smith's home telephone line. A pen register is a device that records all of the numbers dialed from a given telephone line. In this particular case, the pen register captured the robbery victim's phone number being dialed on Smith's telephone line; as a result, a warrant for a search of Smith's home was obtained, incriminating evidence was discovered, and Smith was subsequently convicted of robbery.

Smith appealed, claiming that the use of the pen register violated his Fourth Amendment rights. The Supreme Court disagreed. On the basis of the Katz reasonable expectation test and the results of the Miller case, Justice Blackmun wrote that:

> First, it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes [34].

By 1979, the Court had clearly distinguished privacy rights regarding the content of telephonic communication from the rights accorded to their context. In Section IV-B, we will see how legislators extended this distinction to cover other forms of electronic communication.

B. Information Technology and Legislation

The Electronic Communication Privacy Act (ECPA) of 1986 was passed in an attempt to extend wiretap law to cover all forms of electronic communication [35]. The ECPA includes three titles that provide varying levels of protection for various types of electronic communication:

- Title I: "Electronic Communications in Transit";
- Title II: "Stored Electronic Communication";
- Title III: "Pen Register/Trap and Trace Devices."

Title I covers the "interception and disclosure of wire, oral, and electronic communication"; it is generally understood to cover communication that is actually moving between two points. This title requires that law enforcement agencies obtain a warrant before they can tap a phone or more generally intercept electronic communication that is in transit. § 2518 of Title 1 provides a long list of the information that must be provided by the applicant before a warrant can be authorized, including a statement of facts showing "there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense." It cannot be just any offense—wiretaps can only be authorized in connection with certain types of criminal activity; § 2516 contains a list; it is lengthy, but it is finite.

Title II, sometimes referred to as the Stored Communications Act (SCA), covers stored wire and electronic communications, as well as transactional records. Law enforcement can obtain information covered under this title by providing "specific and articulable facts" showing that the information is "relevant and material to an ongoing investigation" [18 U.S.C. § 2703(d)], a procedural hurdle that is substantially lower than the "probable cause" requirement found in Title I.

Title III, sometimes referred to as the Pen Register Act, covers pen registers and related devices, such as the trap and trace device. A trap and trace device is similar to a pen register, but instead of capturing numbers dialed from a line, it captures the numbers of parties that dial to that line. Title III calls for the minimum protection provided under the ECPA—it is only necessary that an attorney for the Government certify that the requested information is *relevant* to an ongoing investigation:

> Upon an application made under section 3122 (a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation [35, § 3123(a)(1)].

With regard to Title III, it should be noted that certification does not require a magistrate or judge to review the specific facts of the matter, but only whether Title III applies to the requested material, and that the appropriate authority has provided certification.

There has been a great deal of court time spent debating which of the three titles applies to the information collected by cellular networks. This is an important issue, as it determines the legal requirements that law enforcement must meet to obtain the data, and the moral issues that undergird the design of such networks.

Cell site data—a listing of the sites from which cellular registration messages have been received from a given phone—is of particular interest, as it provides detailed location information about the person who carries the phone. From the legal perspective, there are two different categories of cell site data. "Historical" cell site data is a list of the cell sites visited by a subscriber up until the point in time that the request is made. "Prospective" or real-time cell site data is forward looking. A request for

prospective data is a request that the service provider provide a continuous update of the cell sites with which the subscriber has made contact.

The Courts seem to agree that Title II of the ECPA, which covers stored electronic communication, is the appropriate authority for historical cell site data.[14] The basic rationale is that the data have already been stored at the time of the request. There are significant differences of opinion, however, with regard to prospective cell site data. One of the critical legal issues is the question of whether a cellular telephone is considered a tracking device. Several Courts[15] have ruled that a cell phone is not a tracking device and that Title III of the ECPA is the ruling authority. In these cases, the registration messages emitted have been likened to the numbers dialed by the user. As we have noted, the legal protection in this instance is minimal, requiring only that an attorney for the government certify that the information to be obtained is relevant to an ongoing criminal investigation.

Other courts[16] have come to a different conclusion. In 2005, Judge Orenstein of the Eastern district of New York denied a law enforcement request for prospective cell site data. Judge Orenstein found[17] that a cell phone was in fact a tracking device, and that a showing of probable cause was necessary to obtain prospective cell site data. The question may be resolved in the near future; at the time of writing, the question of how prospective cell site data are to be treated under the ECPA is before a federal appellate court in Philadelphia, PA.[18]

The above-cited cases and many, many others show that the presence of information generated by the cellular architecture has motivated law enforcement officials to pursue such information enthusiastically. Use of this technology and other electronic sources of personal information have become appropriated into methods of law enforcement, and such agencies would like to keep the data conduits open. In order to prevent the development of new telephone and other communication technologies from reducing law enforcement's ability to listen in, the FBI sought legislation that would ensure surveillance capabilities for the foreseeable future. The Director of the FBI Louis Freeh made the point quite clearly in testimony before Congress:

> The purpose of this legislation, quite simply, is to maintain technological capabilities commensurate with existing statutory authority—that is, to prevent advanced telecommunications technology from repealing, de facto, statutory authority now existing and conferred to us by the Congress [36].

The resulting legislation—the Communications Assistance for Law Enforcement Act (CALEA) [37]—requires that service providers "facilitat[e] authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service" [47 U.S.C. Section 1002(a)]. CALEA was subsequently amended to cover voice over IP. From a technical standpoint, this means that service providers cannot release IP calls to travel freely between subscriber terminal adapters; instead, the service provider must anchor most calls, creating a fixed point that must be traversed by call packets in both directions.[19] Upon the presentation of an appropriate warrant, duplicate call streams may be generated at this fixed point and passed to law enforcement.

There have been subsequent modifications to ECPA and CALEA, perhaps the most notable being provided through the USA PATRIOT Act.[20] Among many, many other modifications, the PATRIOT Act amended Title II of the ECPA so that stored voice-mail can be obtained by the government through a search warrant rather than through a wiretap order, and expanded the pen register and trap and trace provisions of the ECPA to explicitly cover the context of Internet traffic. The URLs visited from a cellular platform, for example, thus receive the low level of protection provided by Title III of the ECPA.

C. Law and Technology: Conclusions

There are, we believe, two key implications from the above discussion. The first is that if an information networking technology is designed to collect personal information, then that information will become a focus for consumption by various external parties such as advertisers, major corporations, law enforcement agencies, and subsequently the court system. As such, these powerful agents of society seek to keep the door from closing on the extraction of private information, implicating the right to privacy and autonomy about one's individual information. It is in the best interests of fundamental human rights, and

[14]See *In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007) and *In re Application*, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007).

[15]See, for example, *In re Application for an Order Authorizing the Extension and Use of a Pen Register Device*, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007); *In re Application of the United States*, 411 F. Supp. 2d 678 (W.D. La. 2006); *In re Application of the United States for an Order for Prospective Cell Site Location Info.*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (S.D.N.Y. II); *In re Application of the United States of America*, 433 F. Supp. 2d 804 (S.D. Tex. 2006).

[16]See, for example, *In re Application of United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006); *In re Application of the United States of America*, 441 F. Supp. 2d 816 (S.D. Tex. 2006); *In re Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecomm. Records*, 439 F. Supp. 2d 456 (D. Md. 2006).

[17]384 F. Supp. 2d 562 (E.D.N.Y. 2005).

[18]See In The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government, 3d. Cir., 08-4227.

[19]The fixed point often takes the form of a Session Border Controller (SBC). See, for example, "The benefits of router-integrated session border control," White paper, Juniper Networks, http://www.juniper.net/us/en/local/pdf/whitepapers/2000311-en.pdf and http://tools.ietf.org/html/draft-ietf-sipping-sbc-funcs-00.

[20]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, signed into law October 26, 2001.

indeed a moral obligation, then, to limit the collection of such information. This is especially important as individuals' "epistemic power" as Foucault calls it, is limited by ubiquitous surveillance and subsequent winnowing of individuals' abilities for complex epistemological reflection and decision-making. Second, individuals need privacy protection from these powerful agencies, but as laws are generally reactive by nature, the ability of legislatures and courts to protect against privacy invasions that emerge with novel networking technology is limited, and often slow in coming. So, a certain amount of damage will always be done before legislatures or courts can act. It is therefore incumbent upon engineers and computer scientists to minimize the damage that can be done in the first place by embedding privacy awareness in the fabric of their designs. A systematic methodology for doing just this is provided in the next section.

V. PRIVACY-AWARE DESIGN

Having established an obligation to adopt privacy-aware design practices, the question remains as to what such practices would entail. In this section, we present a framework for privacy-aware design. The framework consists of a set of principles that we derived from the Fair Information Practices proposed by the Department of Health, Education, and Welfare (HEW) in a 1973 study entitled *Records, Computers, and the Rights of Citizen* [2]. The results are listed below.

1) Provide full disclosure of data collection:
    1) description requirement;
    2) enforceability requirement;
    3) irrevocability requirement;
    4) intelligibility requirement.
2) Require consent to data collection:
    1) acknowledgement requirement;
    2) opt-in requirement.
3) Minimize collection of personal data:
    1) functional requirement for collection;
    2) distributed processing requirement.
4) Minimize identification of data with individuals:
    1) nonattribution requirement;
    2) separate storage requirement.
5) Minimize and secure data retention:
    1) functional requirement for retention;
    2) security requirement;
    3) nonreusability requirement.

The principles are briefly summarized here. Some of these principles have more technical implications than others—we will focus on the more technical, while only briefly addressing the less technical.

A. Provide Full Disclosure of Data Collection

Disclosure has long been recognized as a critical element of public data collection, and was a prominent component of the Fair Information Practices. We propose that the disclosure of data collection in the specific context of an information network should take the form of a public statement that personal data will be collected, and a full characterization of the type of data to be collected.

A clear and adequate disclosure is important for several reasons. First, it allows the informed user to gauge the extent to which his or her privacy is at risk. It also provides a basis for comparison with other service providers. A basis for comparison, coupled with an informed community of users, creates market pressure for privacy protection. Given that market pressure is one of the greatest threats to privacy, this would be both highly effective and ironic. Finally, the disclosure establishes a contract between the consumer and the service provider. If the contract is breached, then the subscriber has grounds for complaint, and the relevant enforcement agency has a basis for action.

The first element of disclosure is the description requirement. An adequate description includes the type of data to be collected; this should be very specific, including details such as resolution or granularity. For example, cellular systems maintain records of equipment location for the purpose of routing incoming calls to receivers. As we have seen, because of the manner in which these records are kept, cellular systems effectively maintain records of user location. An adequate disclosure of resolution would specify the location granularity: Does the stored location information simply designate the current cell site or a sector within the cell? Or is it as precise as a GPS fix?

There must also be a clear indication as to how long the data will be retained, and the means by which it will be retained. A focus on the means for retention opens the possibility for the advancement of privacy-aware storage technologies (for example, technologies that limit or prevent data reuse, or technologies that allow a subscriber to retain control over his or her data). Informed subscribers may prefer one storage technology to another, motivating operating companies through market forces to adopt the preferred technologies.

Finally, the description should also include the use to which the collected data will be put. Is user location data in a cellular system used exclusively for paging active user equipment, or is it also being used for other purposes?

The effectiveness of a disclosure requirement is strongly dependent on an enforcement requirement. The threat of punishment must be of sufficient magnitude and certainty that a collecting entity will be motivated to provide a clear disclosure and to comply with it. The Federal Trade Commission (FTC) fulfills this role for commercial corporations, enforcing laws that require that companies adhere to their published privacy policies. In a recent case, the FTC took Microsoft to task for allegedly not complying with Microsoft's published privacy policies. A 2002 *New York Times* article [38] quoted a spokesman as saying that the FTC was willing to "take action against companies that don't keep their promises." Local oversight agencies provide similar roles for public utilities. It follows that

enforcement of privacy policies may follow once the corporations and utilities have been motivated to publish privacy policies. Such motivation may take the form of consumer demand or regulation; both entail education of the public and legislators as to the need for disclosure.

It is important that a given data set always be treated according to the privacy policy under which it was collected. As it stands, corporations are free to change their policies at will. For example, both eBay [39] and Amazon.com [40] made changes to their privacy policies that advocacy groups such as EPIC felt significantly reduced customer privacy [41]. An irrevocability requirement should be applied to collected data so that the customer will have some certainty as to how collected data will be treated for the duration of its retention.

The extent to which a subscriber feels secure in his or her communications will lie in part on that subscriber's understanding of the data collection disclosure. It follows that there must be an intelligibility requirement for data collection disclosures. The disclosure has to make sense to an intelligent, but not technically trained user. We recognize that clarity of prose may conflict with legal precision, but it is important to understand that privacy is often a matter of perception; a communication must be understood to be private for there to be a sense of repose and safety, that sense that makes a zone of privacy an important part of an individual's life.

Finally, we turn to the question of accountability: Who is responsible for the disclosure? The responsible organization may be a cellular service operator, utility, bank, or some other entity that is the public face for a given technology. In many cases, however, the service provider or utility may not have complete knowledge of the data collecting capabilities of the underlying equipment. In order for a full and accurate disclosure to be made, organizations that contribute to the development of a given technology must identify data collection on the part of any elements that they develop. This will require a modification of current standardization practices. As new technologies are developed and standardized, standards-making bodies must be responsible for keeping track of the potential for the collection of personal information at all levels. Disclosure thus begins with the design engineers.

B. Require Consent to Data Collection

The term "consent" is loaded with legal implications. Generally speaking, it invokes questions of legal capacity, adequate information and understanding, and voluntariness [42]. For the purposes of privacy protection, consent is the flip-side of disclosure—it establishes the disclosure as a contract. A requirement for consent also serves a pedagogical purpose, as it forces user awareness of the presence of data collection.

We propose that any subscriber/user of a given communication technology must acknowledge the data collection disclosure before they can use the technology. The acknowledgement requirement can take the same form as license agreements for software updates. The user must click an appropriate button on a screen before proceeding to use the technology. Such acknowledgements are also found in car GPS units.

The technology that underlies a given service may change over time. A residential consumer may be associated with a given power utility for a long period of time, during which power consumption monitoring technology has changed dramatically. If data collection practices change, the user should be notified. Furthermore, user consent to such alterations should take the form of an opt-in requirement, as opposed to one of opting out. The former clearly increases the extent to which the consumer understands and acknowledges data collection [43].

C. Minimize Collection of Personal Data

"Personal data" are data that identify or are correlated with the behavior, thoughts, and/or preferences of an individual. For example, one of the authors has shown that residential power consumption data can be correlated with the behavior of individuals within a house; the finer the resolution, the more detailed the disclosure [44]. As noted, telephone networks also collect a significant amount of personal information, including the identities of the parties to conversations (or at least the numbers of the calling and called parties), as well as the location of mobile users. A cellular system effectively tracks subscribers that travel with their cell phones powered on.

The first requirement under this heading is probably the most important of all of the design requirements—it is that such collection be necessary. Specifically, there must be a functional requirement for collection: the collection of personal data must be tied to the functionality of the communication technology. It is not sufficient that such data may be useful for training or testing purposes, or that it could be a lucrative commodity—the data must be provably necessary for the system to work. In the context of a cellular system, for example, it seems clear that a home location register (HLR) must contain sufficient information to route a call to the mobile switching center (MSC) that is closest to the roaming user. It is not, however, necessary that the HLR contain information regarding the most recent GPS location fix, or the identity of the cells traversed over the course of a call. It follows that the functional requirement for collection should not only address the type of data collected, but also, to the extent that it takes the form of a measurement, its resolution.

The distributed processing requirement calls for data to be used as close as possible to the point at which it is collected. There are two rationales for this requirement. First, it prevents the creation of a single database that will be a target for hackers, law enforcement, or others who wish to exploit the data. Second, it reduces the ability of the service provider to market the data to third parties, or to reuse the data for purposes other than that for which it

was originally collected. We will explore this requirement in more detail when we consider privacy-aware demand response systems.

Finally, any data that are collected in bulk for later testing purposes should be aggregated and/or anonymized. It is arguable that the location of user equipment during a call is needed to debug or test a cellular system, but it is clear that there is no need to retain the phone numbers and the identities of the parties to the call.

D. Minimize Identification of Data With Individuals

As we have seen, it is often necessary for the functionality of a telecommunication system to collect information about individual pieces of user equipment. A node B or equivalent entity, for example, has to keep track of the location of a cell phone during a call in order to facilitate handoffs. It is not, however, necessary to associate this location information with an individual, or even with the individual's telephone number. The identities of the parties to a conversation are irrelevant to the problem of maintaining a connection between their telephones.

It follows that there is a distinction to be drawn between collecting information about equipment and collecting information about the equipment's users. The first subrequirement under this heading is the nonattribution requirement, which calls for anonymizing the data collected about equipment wherever possible. For example, when a roaming user registers with a local MSC/VLR, that MSC/VLR needs to authenticate the user with its home HLR. The service provider that operates the MSC/VLR needs to be assured of payment for services. The service provider does not, however, need to know the identity of the user. Authentication procedures can be used to assure the local service provider of payment without providing personally identifying information, as we will see in Section VI-A.

Given that many telecommunication services are billed to individuals, there must be some connection between the usage of the service and personally identifying information, such as a name and address. We propose a separate storage requirement such that billing and "functional" records are stored in separate places. The separation can be enforced through policies of mutually exclusive permissions, such as the Chinese Wall Security Policy. The Chinese Wall Security policy establishes "conflict of interest classes," then puts in place mandatory, legally enforceable controls by which any given individual is allowed to have access to at most one data set belonging to each class [45]. It would thus be both difficult and illegal for any person to have access to both billing and functional records.

We note, however, that with the advent of bulk rates for telecommunication services, it is becoming less necessary to associate a user with a particular instance of service usage. An independent and isolated authentication and authorization authority may be sufficient for future cellular systems.

E. Minimize and Secure Data Retention

Data retention must be directly related to the functionality of the technology. It is not sufficient that data are useful in some other context, or may be useful at some future date. We propose a functional requirement for retention: the storage of the data must be directly connected to the functionality of the technology. As an example, the location of the local MSC associated with a roaming cellular user is necessary for the routing of incoming calls to that user. Outdated location information, however, is of no functional use and should not be retained.

If data must be stored, then it must be protected. The basic security requirement requires that data be stored in such a manner that inadvertent disclosure is difficult or impossible. This is a long-standing, general concern in the telecommunication industry, so we will not dwell on it here except to note that a requirement that consumers be notified when data are lost or stolen has been shown to reduce the frequency of such events.

Finally, but perhaps most importantly, there is a nonreusability requirement that calls for data to be stored in such a manner that its use in an undisclosed manner be difficult or impossible. This is as much a technical/technological problem as one of law or policy. What is being called for is a variation of the cryptographically secure module—hardware that can store and process information, but cannot be forced to provide that information through physical or electronic attack.

VI. CASE STUDIES

In this section, we will consider two case studies in which privacy-aware design practices are applied to information networking. In the first study, we will consider a single problem that is generic to information networking—the need for user authentication—while making an effort to minimize the identification of data with individuals. In this example, we will see that the nonattribution requirement creates a need for tools that will support the practicing engineer in his or her development of privacy-aware systems. In the second example—a privacy-aware demand response system—we will explore several architectural issues, emphasizing the importance of the distributed processing requirement.

A. Anonymous Mobile Authentication

The authentication problem arises in mobile computing and communication networks in many different scenarios, from placing a cellular telephone call to obtaining Internet access in a coffee shop. Put simply, the authentication problem is one of proving to a service provider that you are who you say you are. But if we dig a bit under the surface with a mind towards minimizing the identification of equipment with the individual, we can see that the true nature of the problem from the standpoint of the service provider is ensuring that payment will be received for

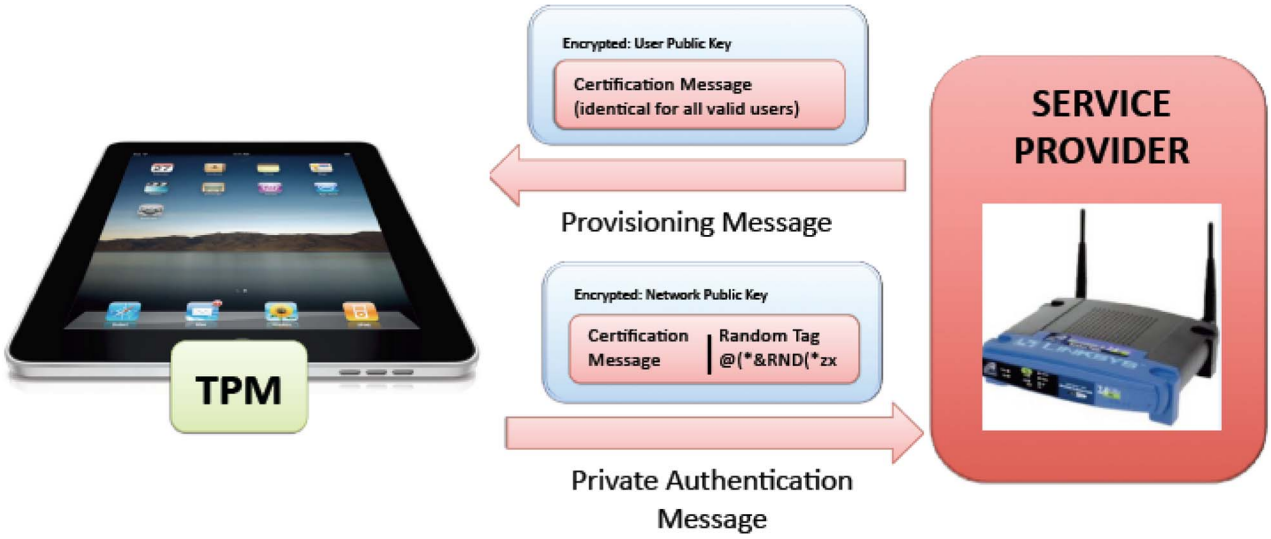

Fig. 1. ***Anonymous authentication.***

services provided. The nonattribution requirement may thus be satisfied—it is not necessary that the service provider know to whom the services are being provided, so long as the guarantee of payment is in place. If anonymous authentication can be established, any data collection entailed by the operation of the service (such as the location data required for the routing of incoming calls to a cellular telephone) will be anonymous.

Anonymous authentication can be characterized as a zero-knowledge proof. The user would like to prove to the service provider that he or she is one of a pool of authorized users, without providing any personally identifying information. One possible solution lies in a scheme developed by one of the authors for the specific application of cellular telephony [46], though it generalizes to a larger context. The scheme is depicted in Fig. 1.

We assume the presence of a public key infrastructure (PKI) that can distribute public keys for the network and its users. The service provider periodically distributes certification messages to all users that are authorized to use the network. The certification message is identical for all users, but is encrypted using each specific user's public key. The encrypted certification message may be transmitted using e-mail, a wireless control channel, or whatever means is appropriate for the application. In some applications, it may be desirable that the certification message not be transferable, in which case a cryptographic vault technology, such as a trusted platform module, can be employed.

When the user wishes to authenticate to obtain service, the certification message is sent back to the network along with a random tag that can be used to identify the equipment. The authentication message is encrypted using the network's public key. Upon receiving this message, the network knows that the user requesting access is valid, as the user knew the certification message. The network does not, however, know the identity of the user. The network can then use the random tag to contact and provide access to the user equipment as needed.

The above is an example of the application of the nonattribution requirement: a system is established by which the network may interact and, if necessary, track the user equipment without knowing to whom the equipment belongs. This design serves to protect moral aspects of privacy for which design architects ought to be responsible: supporting the right to consume privately and anonymously, and as such, the individual is not a target of powerful organizations' panoptic sorting and related moral problems described earlier in this paper. Such a design thus furthers the right to privacy and the self-determination, and keeps open opportunities for developing reflective judgment and decision making. In the next section, we will consider a more involved case study that involves several privacy-aware design principles.

B. Demand Response and Distributed Processing

Utilities are adopting microgrids and other systems that will provide cost savings in power generation, increase grid reliability and flexibility, and create new modes of consumer–utility interaction [47]. Demand response systems will play a key role in this effort. Generally speaking, demand response systems modify electricity consumption behavior by end-use customers in response to changes in the price of electricity over time [48]. The modifications, whether induced by presenting pricing information to the customer or through direct control of appliances by the utility, may alter the timing of demand, the level of instantaneous demand, or the total demand

over a given period of time [49]. The overall goal is to balance electricity consumption over time, alleviating the utilities' (expensive) need to take generators online and offline.

Demand response systems require power consumption information at a level of granularity far finer than that required for monthly billing. The reason is simple: if consumption is to be modified in accord with price over the course of the day, then consumption information must be available at the same level of granularity as the pricing information in order to properly bill the customer. The solution lies in advanced metering infrastructure (AMI)—technology that can sample and record power consumption on a minute-by-minute basis, as opposed to the once-a-month meter readings of the past. AMI deployment has been underway for several years. The Federal Energy Regulatory Commission estimated that there were 7.95 million advanced meters installed nationwide in 2009 [47]. By 2009, 26 utilities in 19 states had announced or pursued advanced metering pilots or full-deployment programs.

The potential impact of demand response is immense. As seen in Fig. 2 (taken from [50]), depending on the extent of the distribution of AMI, the potential savings in energy in the United States during the peak summer period for electrical demand ranges from 4% to 20% of total load. The subsequent positive impact on the United States need for foreign oil and related resources would be difficult to overstate.

Looking more closely at Fig. 2, one can see that the extent of the power savings is a function of AMI participation. An explanation of the various scenarios is provided in Table 1.

In comparing Table 1 to Fig. 2, note that the energy savings from the "opt-in" participation scenario is estimated at 9%, while that of the mandatory, universal approach is 20%. An additional 11% reduction in peak consumption is thus available if regulators require that consumers have advanced metering installed in their homes. This will be an issue of national significance, for unless AMI is employed properly, it poses a serious privacy threat.

In a project supported by the NSF TRUST Science and Technology Center, one of the authors and two colleagues showed that the detailed power consumption data collected by advanced metering systems reveals information about in-home activities. Furthermore, such data can be combined with other readily available information to discover even more about occupants' activities [44]. This result followed from an experiment conducted in a standard student residence (with the appropriate privacy safeguards and the express permission of the resident). An energy usage monitor manufactured was attached to the residence's breaker panel to collect real-time power consumption data. The data, obtained at intervals of 1 or 15 s with a resolution of 1 W, were transferred to a nonintrusive load monitor (NILM) application running on a workstation. A behavior extraction algorithm was then run on the workstation in an attempt to predict behavior based solely on power consumption. Video data were used to establish a control for the experiment.

Some of the results from the experiment are reproduced in Fig. 3. Fig. 3(a) depicts aggregate power consumption data over the course of several days. The vertical axis is labeled in watts, while the horizontal axis depicts the passage of time over the course of several days. There

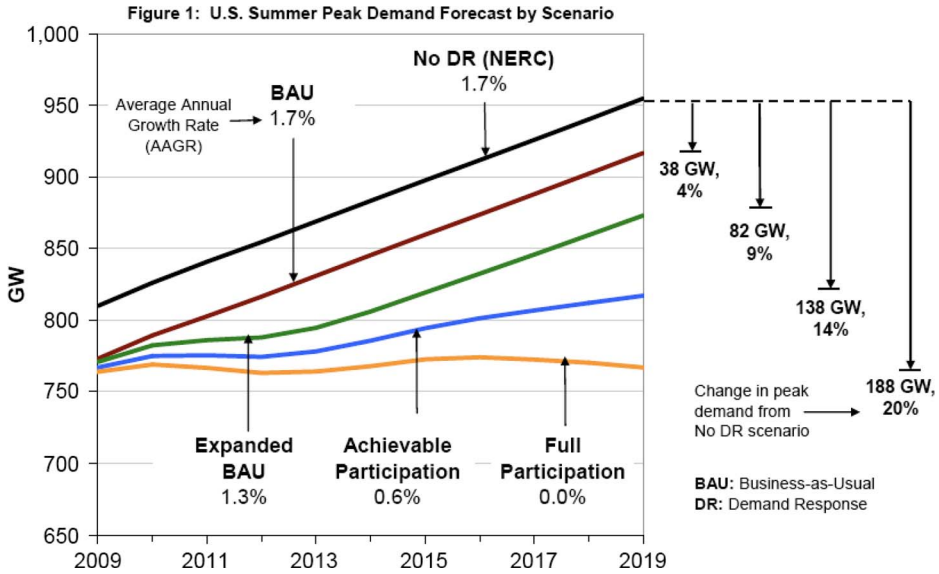

Fig. 2. *Assessment of the potential for demand response [50].*

Table 1 Key Differences in Scenario Assumptions [50]

Assumption	Business-as-Usual	Expanded BAU	Achievable Participation	Full Participation
AMI deployment	Partial Deployment	Partial deployment	Full deployment	Full deployment
Dynamic pricing participation (of eligible)	Today's level	Voluntary (opt-in); 5%	Default (opt-out); 60% to 75%	Universal (mandatory); 100%
Eligible customers offered enabling tech	None	None	95%	100%
Eligible customers accepting enabling tech	None	None	60%	100%
Basis for non-pricing participation rate	Today's level	"Best practices" estimate	"Best practices" estimate	"Best practices" estimate

are several substantial power consumption peaks over the course of each day, indicating activity within the residence.

Fig. 3(b) illustrates the results of an edge detection algorithm applied to the power consumption data collected over several hundred seconds. The edge detection algorithm is quite simple—the graph depicts the difference between power consumption samples that are adjacent in time. The vertical axis depicts $\Delta(t) = P(t) - P(t-1)$, where $P(t)$ is the power consumption sampled at time t. The horizontal axis reflects time. Note that certain switching events can now be isolated—the power consumption transients created by a refrigerator and a microwave oven are easily seen.

Fig. 3(c) is a screen shot taken from a load-identifying program. It shows how events can be isolated and classified

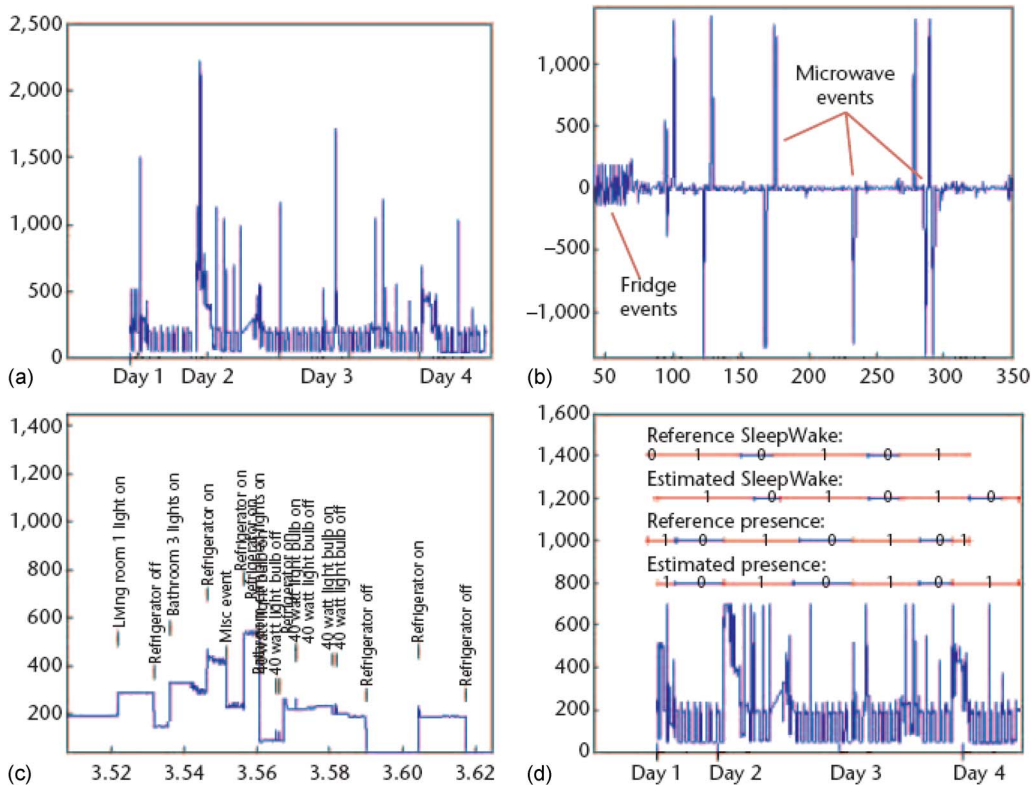

Fig. 3. *Behavior-extraction algorithm. We can see (a) the aggregate power-consumption data, (b) the derived switch events, (c) several identified load events, and (d) a comparison between reference and estimated intervals [44].*

over the course of a day (the units of the horizontal axis is days). With this type of information, we can proceed to estimate the behavior of the individuals within the home.

Fig. 3(d) shows that power consumption data can be used to estimate variables related to personal behavior. The reference lines show actual behavior. On the "Reference SleepWake" line, a zero indicates that the occupant was asleep; a one indicates that he was awake. On the "Reference presence" line, a zero indicates that the occupant of the residence was not at home; a one indicates that he was at home. The estimated lines indicate our estimates of these events. Note how close the reference data are to the estimates.

Given that power consumption data creates a privacy problem, it is clear that centralized collection may prove unsettling to customers of the utilities that implement it. Yet centralized collection would appear to be the direction being taken. In the following excerpt from the 2006 FERC "Assessment of Demand Response and Advanced Metering," AMI is *defined* as a system that provides for centralized collection. There seems to be no allowance for architectural options that are more sensitive to the privacy needs of the consumer.

> For purposes of this report, Commission staff defined "advanced metering" as follows: "Advanced metering is a metering system that records customer consumption [and possibly other parameters] hourly or more frequently and that provides for daily or more frequent transmittal of measurements over a communication network to a central collection point" [53].

The above definition has since been quoted by utilities.[21] It has also been represented graphically in AMI literature distributed by FERC, as seen in Fig. 4 [51]. Note that reference is made to the potential for third party data reception and management. This arguably increases the potential for unregulated use of the acquired data, including commodification and subsequent reuse by marketers and others.

The long-term future of the demand response program may be at risk. Consumers may become alarmed at the potential invasion of privacy, motivating legislation calling for an expensive retooling of the system. Judicial action may also put the program at risk. Whether from public outcry or judicial action, systems that forsake privacy awareness may find themselves shut down.

When we view demand response systems through the lens of privacy-aware design, however, a privacy-preserving solution is apparent. The goal of demand response systems is to modify consumption behavior,

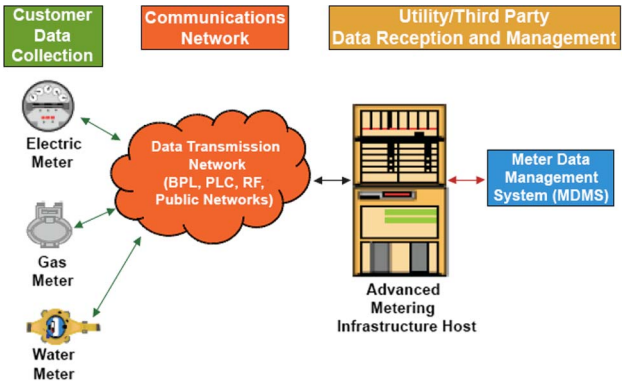

Fig. 4. ***AMI building blocks [51].***

whether through inducement or direct control, by exploiting fine-grained pricing information. The behavior of interest—consumption—is highly distributed. With the distributed processing requirement in mind, it becomes clear that it is not the power consumption data that need to be collected, but it is instead the pricing data that need to be distributed. Fine-grained consumption information need never leave the immediate neighborhood, thus alleviating most privacy concerns.

A privacy-aware demand response architecture must account for several different data flows. For each of them, a privacy analysis should be performed and a privacy-aware design adopted as necessary. First, in systems that seek to alter consumer behavior, pricing data must be presented to the consumer so that he/she has a basis upon which to make consumption decisions. This does not present a privacy concern, as the utility can simply broadcast the pricing to the residential meter and/or to an application on the consumer's home computer.

Second, in direct control systems, the utility has to send signals to appliances to control their electricity consumption over the course of the day. Though this may create a significant security issue, it does not provide information about consumer behavior and preferences within the home.

The third flow is more problematic. Consumer-specific consumption data must be provided to the utility for billing purposes. There is an issue here, as one cannot stream consumption data to the utility without creating the aforementioned privacy issue. One also cannot stream real-time cost data, as it would be trivial to convert this information back into consumption data. The solution lies in accumulating price-weighted consumption data at the residence and then sending the aggregate cost to the utility on a weekly or monthly basis. This implies a level of security at the meter that requires a trusted platform module or the equivalent.

Finally, the utility needs consumption data, temporally precise, but aggregated at the level of the consumer, in

[21]Illinois Smart Grid Initiative Final Report, "Empowering consumers through a modern electric grid," 2009, p. 14. Available at: http://www.cnt.org/repository/ISGI.FinalReport.pdf.

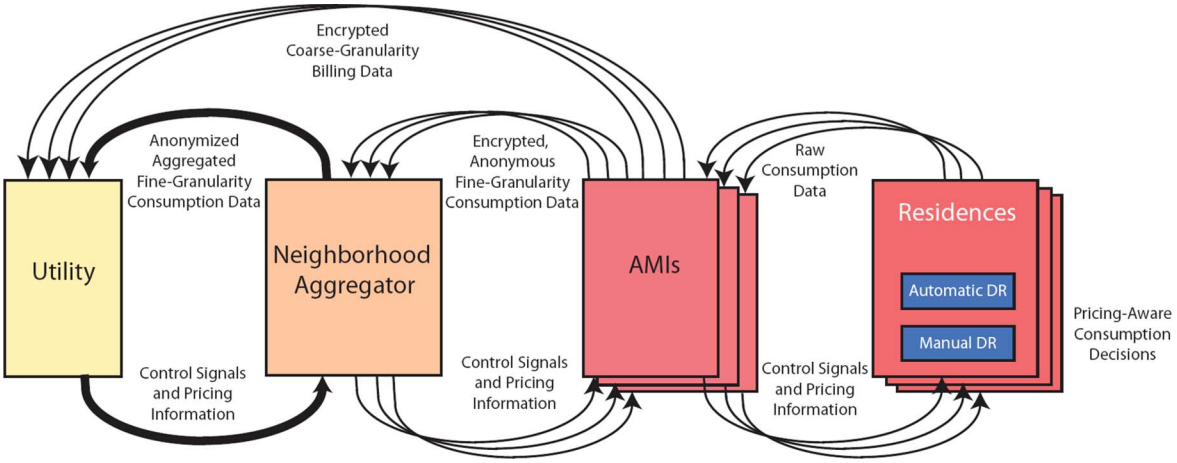

Fig. 5. ***Privacy-aware demand response architecture.***

order to predict demand and maintain a price model. Typically, aggregated real power consumption data at the substation level are sufficient to predict the need for new transmission and distribution lines and generation necessary to service the predicted demand. A neighborhood aggregator can be used to combine and anonymize data so that the desired temporal granularity is provided without generating information about individual behavior. Anonymization can be performed by summing the power consumption data for a sufficient number of customers so that a single customer's data cannot be isolated.

The above solutions are embedded in the architecture depicted in Fig. 5.

VII. CONCLUSION

In this paper, we have established a moral and ethical obligation for the use of privacy-aware engineering design practices. We provided a survey of the literature on the nature of privacy, and then briefly explored the means by which social scientists have characterized the impact of privacy invasion. We then exposed a moral hazard—the lucrative uses to which marketers can put personally identifying information, and the hazard of the deflection of individual autonomy and related cognitive implications of compromised decision making abilities and curtailed epistemic development. The protection provided by case law and legislation was then discussed, emphasizing the distinction that has been drawn between the content and the context of electronic communication. A framework for privacy-aware design practices was then developed as a roadmap for embedding privacy awareness into information networks, and implicating the necessity for design architects to be aware of the moral, epistemic, and legal consequences that nonrestricted designs engender. The framework was then applied to the problems of mobile authentication and the collection of power consumption data for demand response systems.

In closing, we wish to emphasize that privacy-aware design is still in its infancy. There are many interesting technical problems to be solved as the design toolbox for privacy-aware information networks is developed. The benefit to the individual and society that stems from such an effort will, we hope, be highly motivating and rewarding. ■

REFERENCES

[1] K. J. O'Brien, "Europe pushes Google to turn over Wi-Fi data," *New York Times*, Jun. 27, 2010.

[2] HEW, *Records, Computers, and the Rights of Citizen*, 1973.

[3] F. D. Schoeman, *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, U.K.: Cambridge Univ. Press, 1984.

[4] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Rev.*, vol. 4, pp. 193–196, 1890.

[5] T. M. Cooley, *A Treatise on the Law of Torts*,2nd ed. Chicago, IL: Callaghan, 1888, p. 29.

[6] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Rev.*, vol. 79, pp. 119–158, 2004.

[7] J. Cohen, "Examined lives: Informational privacy and the subject as object," *Stanford Law Rev.*, vol. 53, pp. 1373–1437, 2000.

[8] M. Hindman, *The Myth of Digital Democracy*. Princeton, NJ: Princeton Univ. Press, 2008.

[9] O. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview, 1993.

[10] J. S. Mill, *On liberty*, 1859.

[11] A. Finder, "For some online persona undermines a résumé," *New York Times*, Jun. 11, 2006.

[12] J. Bentham, *The Panopticon; or, The Inspection House (1787)*, M. Bozovic, Ed. London, U.K.: Verso, 1995.

[13] M. Foucault, *Discipline and Punish*. New York: Vintage, 1995, (English translation; the original French version

is *Surveiller et punir: Naissance de la Prison*, Paris, France: Gallimard, 1975).

[14] M. Foucault, "Truth and judicial forms," in *Power: The Essential Works of Michel Foucault 1954–1984*, vol. 3, J. Faubion, Ed. New York: New Press, 2000, pp. 83–84.

[15] P. King and K. Kitchener, *Developing Reflective Judgment: Understanding and Promoting Intellectual Growth and Critical Thinking in Adolescents and Adults*. San Francisco, CA: Jossey-Bass, 1994.

[16] M. Foucault, *Je suis un artificier*, R.-P. Droit, Ed. Paris, France: Odile Jacob, 2004, p. 106. [Online]. Available: http://www.michel-foucault.com/

[17] *The Power of Direct Marketing: ROI, Sales, Expenditures and Employment in the US*, 2009–2010 ed., DMA, New York.

[18] J. B. Rule, *Privacy in Peril*. Oxford, U.K.: Oxford Univ. Press, 2007.

[19] "Austin TX police have access to Austin Energy customer accounts," *Over the Line, Smokey*, Nov. 7, 2007. [Online]. Available: http://seesdifferent.wordpress.com/2007/11/07/austin-tx-police-have-access-to-austin-energy-customer-accounts/

[20] "infoUSA to purchase Donnelley marketing from First Data Corporation—First Data Corporation's President & COO to join infoUSA board," *Business Wire*, Jun. 1, 1999.

[21] E. Steel and J. Angwin, "On the web's cutting edge, anonymity in name only," *Wall Street J.*, Aug. 4, 2010.

[22] L. Coe, *The Telegraph: A History of Morse's Inventions and Its Predecessors in the United States*. Jefferson, NC: MacFarland, 1993.

[23] S. Dash, R. Schwartz, and R. Knowlton, The Eavesdroppers. New Brunswick, NJ: Rutgers Univ. Press, 1959.

[24] *Sacramento Daily Union*, p. 2, Aug. 12, 1864, column 4.

[25] "Washington.; Secrets of the telegraph. Private telegraphic correspondence. No longer inviolable a house committee prowling over a ton of dispatches," *New York Times*, p. 4, Jun. 24, 1876.

[26] J. Brooks, *Telephone, The First Hundred Years*. New York: Harper Collins, 1975.

[27] "Seymour wires tapped on order given by Woods," *New York Times*, p. 1, May 18, 1916, column 1.

[28] *Opinon of Chief Justice Sir John Fineux*, Yearbook, Michelmas, 21 Henry VII 39 (K. B. 1505).

[29] Eng. Rep. 194, *Semayne's Case*, Coke's Rep. 91a, 77 Eng. Rep. 194 (K.B. 1604).

[30] *Paxton's Case*, Gray, Mass. Repts., 51 469, 1761.

[31] Olmstead v. United States, 277 U.S. 438, 1928.

[32] Katz v. United States, 389 U.S. 347, 1967.

[33] United States v. Miller, 425 U.S. 435, 1976.

[34] Smith v. Maryland, 442 U.S. 735, 1979.

[35] *Electronic Communications Privacy Act*, 18 U.S.C. §§ 2510-21, 2701-11, 3121-3127.

[36] L. J. Freeh, *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services*, Joint Hearings on H.R. 4922 and S. 2375, 103d Cong. 7, 1994.

[37] USC 47, Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010.

[38] J. Schwartz, "Settling with F.T.C., Microsoft agrees to privacy safeguards," *New York Times*, Aug. 9, 2002.

[39] J. Kornblum, "Changes to eBay may put customer info at risk," *USA Today*, Feb. 27, 2002. [Online]. Available: http://www.usatoday.com/tech/news/2002/02/28/ebrief.htm

[40] P. Jacobus, "Privacy groups call Amazon policy 'deceptive'," *CNET News*, Dec. 4, 2002. [Online]. Available: http://news.cnet.com/Privacy-groups-call-Amazon-policy-deceptive/2100-1017_3-249376.html

[41] K. Regan and C. Saliba, "Privacy watchdogs blast amazon," *E-Commerce Times*, Sep. 14, 2000. [Online]. Available: http://www.ecommercetimes.com/story/4283.html?wlc=1272369148

[42] C. W. Lidz, *Informed Consent: A Study of Decision Making in Psychiatry*. New York: Guilford, 1984.

[43] J. Sovern, "Opting in, opting out, or no options at all: The fight for control of personal information," *Washington Law Rev.*, vol. 74, pp. 1033–1130, 1999.

[44] M. Lisovich, D. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security Privacy Mag.*, vol. 8, no. 1, pp. 11–20, Jan./Feb. 2010.

[45] D. F. C. Brewer and M. J. Nash, "The Chinese wall security policy," in *Proc. IEEE Symp. Security Privacy*, 1989, pp. 206–214.

[46] S. B. Wicker, "Digital telephony and the question of privacy," *Commun. ACM*, to be published.

[47] Federal Energy Regulatory Commission. (2009, Sep.). 2009 Assessment of demand response and advanced metering, Staff Rep. [Online]. Available: http://www.ferc.gov/legal/staff-reports/sep-09-demand-response.pdf

[48] M. H. Albadi and E. F. El-Saadany, "A summary of demand response in electricity markets," *Electric Power Syst. Res.*, vol. 78, pp. 1989–1996, 2008.

[49] OECD, *International Energy Agency, The Power to Choose—Demand Response in Liberalized Electricity Markets*, Paris, France, 2003.

[50] Federal Energy Regulatory Commission. (2009, Jun.). A National assessment of demand response potential, Staff Rep. [Online]. Available: http://www.ferc.gov/legal/staff-reports/06-09-demand-response.pdf

[51] Engineering Power Research Institute, *Advanced Metering Infrastructure*. [Online]. Avaiable: http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf

[52] O. S. Kerr, "Internet surveillance law after the USA Patriot Act: The big brother that isn't," *Northwestern Law Rev.*, vol. 97, pp. 607–611, 2003.

[53] Federal Energy Regulatory Commission, "Assessment of demand response and advanced metering," Washington, DC, Staff Rep., Docket No. AD06-2-000, Aug. 2006, p. vi.

[54] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford Univ. Press, 2010.

ABOUT THE AUTHORS

Stephen B. Wicker (Fellow, IEEE) received the B.S.E.E. degree from the University of Virginia, Charlottesville, in 1982, the M.S.E.E. degree from Purdue University, West Lafayette, IN, in 1983, and the Ph.D. degree from the University of Southern California, Los Angeles, in 1987, all in electrical engineering.

Currently, he is a Professor of Electrical and Computer Engineering at Cornell University, Ithaca, NY, and a member of the graduate fields of Computer Science, Information Science, and Applied Mathematics. As of mid-2010, he has supervised forty doctoral dissertations. He teaches and conducts research in wired and wireless information networks, digital systems, and privacy-aware design practices. He is the Cornell Principal Investigator for the TRUST Science and Technology Center—a National Science Foundation center dedicated to the development of technologies for securing the nation's critical infrastructure. He was recently selected to serve on the Air Force Scientific Advisory Board. He is the author of *Codes, Graphs, and Iterative Decoding* (Norwell, MA: Kluwer, 2002), *Turbo Coding* (Norwell, MA: Kluwer, 1999), *Error Control Systems for Digital Communication and Storage* (Englewood Cliffs, NJ: Prentice-Hall, 1995) and *Reed-Solomon Codes and Their Applications* (Piscataway, NJ: IEEE Press, 1994).

Prof. Wicker was awarded a 1998 Cornell College of Engineering Teaching Award, the 2000 Cornell School of Electrical and Computer Engineering Teaching Award, and a 2009 Cornell College of Engineering Teaching Award. He has served as an Associate Editor for Coding Theory and Techniques for the IEEE TRANSACTIONS ON COMMUNICATIONS, and is currently an Associate Editor for the *ACM Transactions on Sensor Networks*. He served two terms as a member of the Board of Governors of the IEEE Information Theory Society.

Dawn E. Schrader received the B.A. degree in sociology from Miami University, Oxford, OH, in 1979, the M.A. degree in education from The Ohio State University, Columbus, in 1982, and the Ed.D. degree in human development from Harvard University, Cambridge, MA, in 1988.

Currently, she is an Associate Professor of Psychology in Education at Cornell University, Ithaca, NY. She is a member of the Cornell University graduate fields of education, human development, and cognitive science. As a research psychologist and educator studying morality and ethical reasoning, her work addresses the psychological processes moral development, decision-making, reflection, and action. She studies these processes across the contexts of social and personal relationships, educational institutions, and professional education. She developed the action–judgment–awareness (AJA) model that consists of three dynamically related components: action—the real life choices and experiences of persons; judgment—the psychological frameworks that people currently use; and awareness—the metacognitive, reflective, and conscious awareness of thoughts, strategies, experiences, and situational/contextual demands. Combined together, individuals can develop more effective and ethical strategies for dealing with complex moral issues. She publishes and presents nationally and internationally on cognitive moral psychology and education, and is coauthor of the upcoming book, with Ewa Nowak, *Educating Competencies for Democracy* (Rotterdam, The Netherlands: Sense Publishers, in preparation).

Dr. Schrader received the State University of New York's Chancellor's Award for Excellence in Teaching, and numerous other teaching awards from the Mortar Board Society, Quill and Dagger, and Panhellenic and Interfraternity Councils, among others, at Cornell. An active researcher and scholar, she serves on the Executive Board of the Association for Moral Education, the Advisory Board of Girls Learn International, and is cofounder of the Society for Research in Adult Development.