Communications of the Association for Information Systems

Volume 36 Article 2

1-2015

Anonymity vs. Security: The Right Balance for the Smart Grid

Sanjay Goel
University at Albany, SUNY, goel@albany.edu

Communications of the Association for Information Systems

CAIS

Anonymity vs. Security: The Right Balance for the Smart Grid

Sanjay Goel

Associate Professor and Chair, Department of Information Technology Management, School of Business, University at Albany, State University of New York

Director, Center for Forensics Analytics Complexity Energy Transportation and Security (FACETS)

goel@albany.edu

Abstract:

This paper examines the conflict between anonymity and security in the context of new innovations that leverage the Internet. Anonymity affords an opportunity for the marginalized to express opinions without fear of persecution or discrimination; however, anonymity also facilitates crime and fraud. Its antithesis, traceability, is meant to deter malicious behavior, but can also be used by governments to control and persecute their populations. The debate between anonymity and security on the Internet is intricately intertwined with threats to domestic and international security. As we launch into the implementation of the Smart Grid, arguably the largest engineering project of modern times, it is time to reexamine the fundamental premises on which the Internet was constructed. A single Internet may no longer be able to handle the conflicting demands of different applications. A new Internet with rules that balance security and anonymity may be appropriate for Smart Grid and other similar critical infrastructure projects. I present the rationale of rethinking the design of the Internet that simplifies its architecture, reduces its complexity, and removes vulnerabilities that have been exploited persistently. I also discuss some of the current trends, especially those related to standards and guidelines on Smart Grid privacy and security.

Keywords: Smart Grid, Anonymity, Privacy, Fourth Amendment, Privacy Regulations, Electric Grid.

Volume 36, Article 2, pp. 23-32, January 2015

The manuscript was received 16/02/2013 and was with the authors 12 months for 3 revisions.

I. INTRODUCTION

Many people do not realize how inextricably their lives depend on electricity until there is a blackout. Today's fragile electric grid runs to capacity in several places with obsolete equipment. One of the largest engineering challenges today is modernizing the electric grid to make it more resilient and efficient. This effort will result in an intelligent electric grid with the ability to recover from faults autonomously through use of sensors and automated relays. This redesigned grid is being termed the smart grid. The smart grid leverages information and communication technology extensively for achieving resilience and efficiency. Operationally, the smart grid superimposes the communication grid on top of the power grid to enable extensive data collection and analysis. In the near future, it will connect millions of electric meters, relays, power stations, and generators into a single network that controls power transmission, distribution, and usage. This extensive data collection will provide operators with the ability to monitor the grid, to accurately pinpoint (and even self-correct) any faults, and to fine tune the grid for improved operational efficiency. This massive effort has three primary initiatives: that is, 1) adding sensors throughout the network, 2) allowing two-way metering, and 3) adding demand-response capability. Sensors in the network allow for monitoring and building resilience in the grid. Two-way metering allows micro energy generation sources at individual household level to be integrated into the grid. Demand-response allows utility companies to manage load variability by actively controlling electricity usage at an appliance level in households. In the past, the variability was managed by increasing and decreasing electricity supply through fast starting generators, which is very expensive. All of these functions are intricately dependent on information and communication technologies (ICT). This intricate dependence on ICT also makes it a potent target for attacks from multiple actors including criminals, terrorists, and nation states. Obviously, the power grid is an essential element of a country's critical infrastructure and needs to be both secure and reliable. The smart grid would be the largest network of physical nodes in size after the Internet, and could even grow to surpass it. In designing the smart grid, two questions emerge: (1) does the smart grid need to be part of the existing monolithic Internet?, and (2) should the same ideals (e.g., anonymity, privacy, and uniformity) that apply to the Internet guide the smart grid's construction?

While the Internet is being used as a blueprint for designing the smart grid, its implementation should consider the lessons learned in the past to avoid any unnecessary pitfalls. History has shown that humans tend to repeat the same mistakes time and again, and such errors with the smart grid would have grave consequences, especially since cyber warfare is becoming the next arena for international conflict. The smart grid would be a prime target for cyber-attacks during conflict since power failures can have serious economic and psychological consequences on the attacked country. An intuitive first step would be to examine the basic assumptions on which the Internet was initially created and ask ourselves if these same assumptions are relevant considering the Internet evolved into a complex entity in an attempt to balance conflicting requirements. We need to think of unconventional, novel ideas that will radically change the existing paradigm. Were the assumptions inadequate, we would need to rewrite them to fit better with today's realities. The fact that the Internet is, essentially, a single monolithic network that caters to multiple applications with conflicting needs is a severe limiting factor. One possible solution would be to create different internets for specific purposes. What would be the ramifications of creating a parallel Internet with a different set of assumptions more suited for the smart grid?

In this paper, I examine the basic tenets on which the current Internet was developed and examine its implication on for the smart grid. The paper is organized as follows: in Section 2, I describe the smart grid and discuss in-depth its data storage, security, and anonymity requirements. In Section 3, I discuss the anonymity dilemma in relation to personal freedom and security on the Internet at a holistic level. In Section 4, I discuss the changing needs of the Internet and provide thoughts on addressing the security vs. anonymity dilemma. In Section 5, I conclude the paper.

II. SMART GRID

Multiple failures or significant oscillations in voltage and phase can cause failures that cascade into large-scale blackouts, as evidenced in the Northeast Blackout in 2012. The fact that the power grid is overstressed in places is evident from the widespread blackouts that occurred in North America and Europe in 2010 and in India in 2012. The current method of balancing supply and demand in the grid (to avoid voltage drops and power surges) is inefficient and requires constant interaction between generators and grid operators. The design of the grid is very utility centric, which makes it difficult to incorporate alternate energy sources such as wind and solar into it (Goel, Bush, & Bakken, 2013). Efforts to integrate alternative energy sources (e.g., solar, wind, and wave power) into the grid complicate our ability to achieve a stable balance due to the variability and unpredictability of these sources. Finally, grid

synchronization (i.e., efforts to ensure that the phases of the current are aligned to prevent power loss) needs to be vastly improved in order to prevent interruptions in supply. With smart grid, the goal is to improve the grid's stability and reliability and, at the same time, enable new functionality to facilitate the incorporation of distributed renewable sources.

This smart grid is envisioned as an interconnected power distribution network that streamlines the transmission, distribution, monitoring, and control of electricity. In order to achieve this interconnectivity, the smart grid fundamentally alters the grid's architecture by blurring the boundaries between generation, transmission, and distribution to create a single monolithic grid. At the most basic level, one can view the electric grid as a large complex network composed of interconnected power plants, electricity distribution infrastructure, and consumers interspersed across national and international borders. Technologically, one can view the smart grid as a superposition of the Internet on the electric grid (Goel et al., 2013). Grid efficiency stems from the ability of the information network to allow efficient operation of the grid by reducing the latency of information in it. While the current grid allows only a one-way communication and flow of power, the smart grid will allow for two-way communication and two-way flow of power. Generally, consumers only draw power from the electric grid. In the future, greater numbers of consumers will supply power back to the grid through solar panels, windmills, or even stationary bikes that can be used for both exercise and power generation. With smart grid, the goal is thus to address three key issues: (1) the grid's fragility, (2) load-balance on the grid, and (3) difficulty in integrating renewable micro-energy sources in the grid. Smart grid implementation has several other objectives, which include increasing competition between providers, improving transmission reliability, and enabling market forces to drive consumption. The smart grid's success rests in its ability to provide ubiquitous, secure communication throughout the grid. This will allow data to be collected, analyzed, and interpreted for decision making in order to achieve the goals set for it. An information network will be overlaid on the conventional power grid; this integrated network will collect data, manage the grid, and keep track of power failures and, thus, revolutionize the way the grid functions. In building the smart grid, we need to answer the following questions: What data will the communication network carry? What security requirements need to be imposed on this network? What is the importance of anonymity and privacy on this network?

Smart Grid Data

The smart grid will carry two kinds of data: 1) two-way electricity metering data, and 2) diagnostic and state data from sensors placed on the grid. Metering data are collected from individual consumers for demand prediction, billing, and demand response. Diagnostic data on the network comes from sensors in the grid that are used to detect faults on it so that they can be isolated with reclosers, and state data will come from special sensors called synchrophasors, which measure the characteristics of electric waves on the grid using a common time source for synchronization. The volume of data being collected will increase dramatically with the smart grid. For instance, utilities currently collect one monthly reading per customer. If they start collecting information each minute with the smart grid, the monthly reading per customer will grow to over 43,000 readings. The data collected from sensors will increase even more drastically as we attempt to gain visibility into the grid and will make transmitting, storing, and analyzing data a huge challenge.

Security and Anonymity in the Smart Grid

Data integrity is extremely important since data manipulation could not only lead to customer inconvenience but also to instability and disruptions in the grid. The smart grid is quite vulnerable to data spoofing attacks, which includes transmitting false sensor data, disabling relays, disrupting load balance, and inducing faults. Diagnostic data corruption could drastically hurt disaster recovery if utility crews are misdirected to phantom faults. State data allows corrections to operational variables in the grid to ensure it is maintained in a narrow range of state parameters for maximum efficiency. If this data were manipulated, the grid controllers could react to false readings and make corrective actions that can destabilize the grid. There are clear needs for integrity since data tampering could result in metering fraud, large-scale metering fraud, and the undermining of operators' efforts to balance the grid. Any such weakness can be exploited by terrorists and cyber nation states alike, who can deploy hacking tools, including malware, to cripple the network. Availability is also important since data are required in real-time for operational needs, and failure to obtain information can lead to degradation of performance and, in a worst case scenario, data from critical sensors or SCADA systems during crisis conditions can lead to cascading failures.

Importance of Anonymity in the Smart Grid

With the smart grid, the metering data collected will become much more precise; user behavior could be easily inferred from electricity usage patterns. Anonymity is primarily associated with this metering data, which is time-series data, required for accurately predicting demand in the short term and for computing consumer electricity usage for billing based on time of use. In the past, electric meters only aggregated usage and charged the same price irrespective of time of power use even though prices vary significantly from region to region. Each appliance

has a unique electricity usage signature; by analyzing the overall usage signature, the usage of different appliances can be easily determined (i.e., what appliances people are using and at what time of the day). This information can reveal individual's lifestyle, which can be used for target marketing, discrimination (e.g. in insurance and employment), evidentiary purposes in lawsuits, and even committing crimes, such as, robbery, kidnapping, and stalking. Data needs to be secured; however, metering data needs to be associated with specific consumers for billing, obviating the need for anonymity. This raises the question of how much data can be collected before individual freedom and security are threatened. There are precedents from Internet that we can draw on to understand the problem better.

The issues related to managing large volumes of data and their integrity and availability are primarily technical issues that can be largely addressed by technical means that include increasing storage and computing capacity, integrity checks, redundant communication media, fallback decision rules in duress conditions, and so on. There are issues of privacy and anonymity that are fundamentally different and that impact the user and need a deeper analysis that goes to the core of constitutional rights and to the fundamentals of the Internet's design (Leiner et al., 1997). I discuss this in depth in Section 3.

III. ANONYMITY AND PRIVACY ON THE INTERNET

The Internet has greatly encouraged access to information and freedom of expression worldwide. The Internet both reflects and influences societal norms and can be a great equalizer. Several well-known Internet activists have strongly argued for freedom on the Internet and net neutrality (Wu, 2003; Lessig & McChesney, 2006; Berners-Lee, 2010). This freedom is also considered an anathema to political stability because it allows actors inimical to governments to express their views, foment unrest, recruit followers, and communicate anonymously (Tufekci, 2011). The balance between security and freedom constantly shifts in response to perceived threats. In times of war, individuals often give up personal freedoms for the sake of national security. The United States, in wake of the September 11, 2001 attacks on New York and Washington DC, enacted new legislation that greatly restricted personal freedoms and expanded government powers of surveillance in the name of national security[1]. Countries all over the world began to control Internet content in the aftermath of the revolutions in the Middle-East that led to the ousting of several regimes; these revolutions seem to be catalyzed by protests coordinated over social media (Axford, 2011; Eltantawy & Wiest, 2011; Comunello & Anzera, 2012). The balance between security and freedom is not necessarily an inverse relationship (where maximizing one will minimize the other) but rather a multimodal space where security can be increased without necessarily having a negative impact on freedom (Verzi & Coates, 2004).

There has been sustained debate over anonymity on the Internet since its inception. Anonymity is important' however, it is also a limiting constraint in ensuring security. Anonymity and privacy are often used interchangeably, but are not synonymous. Something done anonymously remains unattributed to a known actor even if the act itself is made public. Something done privately is intended to be known only by a limited group of trusted parties. Free speech on the Internet is facilitated by anonymity[2], which allows individuals to express their views openly without fear of persecution or discrimination. Internet privacy (Cranor, 1999), on the other hand, restricts access to information to a specific individual or a group of predetermined individuals; it is facilitated by the use of encryption techniques and related technologies (Bonneau & Preibusch, 2010). I discuss the issue of anonymity in the following two subsections, and subsequently discuss privacy and the balance between privacy and anonymity.

Need for Anonymity

Several potent arguments for anonymity on the Internet exist; these, in essence, boil down to protecting individuals from persecution, discrimination, and embarrassment. Anonymity allows religious, ethnic, and political minorities to express their opinions openly without fear of retribution or discrimination by a more-powerful majority. This is extremely significant in countries without a culture that protects or promotes freedom of expression and where the media are tightly controlled or censored. The Internet provides a vital online forum which, in some instances, leads to profound impacts. Online assemblies played a pivotal role in cultivating successful revolutions in Egypt, Libya, and Tunisia, and in the failed attempts to instigate reform in Iran and in the ongoing conflict in Syria. These successful and failed revolution attempts were not caused by the Internet, but were certainly facilitated and perhaps even catalyzed by it.

Consequently, the Internet's freedom and anonymity, which are cherished and espoused in many democratic countries, are often considered anathemas in societies where social beliefs and political realities are circumscribed by undemocratic or theocratic regimes. Leaders who view exposure to outside opinions as threats to their cultural

[1] HR 3162. USA PATRIOT Act: Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism
[2] Freedom on the Internet has several connotations including privacy, the right to assemble, anonymity, and freedom of speech. My main focus in this paper is on anonymity.

and religious traditions have found creative ways to limit Internet access to preserve vested interests. Nations that attempt to restrict freedom of speech on the Internet rely on legislation, technical means (Internet filtering, account disablement), and coercion. Even open, democratic governments elect to engage in some form of Internet censorship to protect national interests and prevent crime. Anonymity is also important because it enables users to discuss personal problems and seek help anonymously from the Internet community at large in societies that can be conservative and judgmental. These communities include groups for people of different sexual orientation, workplace discrimination advice, medial issue discussion, and debates on race and minority issues.

Downside of Anonymity

While anonymity can be beneficial in protecting personal freedom, it may also camouflage criminal behavior. Money laundering, drug trafficking, terrorism, hacking, fraud, child pornography, hate crimes, and bullying are all perpetrated through and facilitated by the Internet (Armstrong & Forde, 2003). The Internet allows terrorists to share their ideology with a wider population than ever before and to recruit individuals bent on revenge and martyrdom. The ability to recruit local volunteers in New York, London, or Paris rather than transporting supporters from abroad can be a significant tactical advantage. Home-grown terrorists have committed attacks in Egypt, India, Indonesia, Pakistan, Russia, Spain, the UK, and the US. The Internet allows terrorists to create distributed, layered, and resilient organizations and to exercise considerable influence on the flow of information, public opinion, and politics across the globe.

Balance Between Anonymity and Security

Terrorist attacks in New York, London, and Madrid all led to public outrage and demands for greater security. Each country differed, however, in terms of how it chose to balance these demands with the protection of personal freedom. The USA-PATRIOT Act[3] was enacted several weeks after the September 11, 2001 attacks and permitted law enforcement agencies unprecedented access to U.S. citizens' phones, emails, medical records, financial records, and other types of information; the Patriot Act also broadened the discretion of law enforcement and immigration authorities to detain and deport immigrants suspected of terrorism-related activities. This and related legislation gave authorities the right to conduct warrantless surveillance. Various countries also adopted international legislation that supports information sharing among themselves and defense activities against terrorist acts (e.g., United Nations Security Council Resolution 1368[4]) in the wake of September 11th, 2001. While there have not been any large-scale attacks on American soil since that time, there are many who would argue that the U.S. Government overreacted. Many of the activities permitted by the USA-PATRIOT Act were meant to be phased out in 2005, but were instead reauthorized; power granted to law enforcement officials to hunt down terrorists has, in some cases, been misused for political purposes, personal vendettas, and human rights violations. We are faced with the task of trying to protect privacy and personal freedom on the Internet while ensuring that law enforcement and intelligence officials obtain the information needed to track down criminals and terrorists.

Even at a personal level, the concept of privacy can vary significantly across individuals. Breaches of sensitive personal information can result in embarrassment and discrimination; however, an ever larger number of individuals freely choose to disclose personal information on social networking sites such as Facebook (Albrechtslund, 2008). Privacy is thus an extremely subjective concept. Acquisti and Grossklags (2007), moreover, argue that we worry about insignificant invasions of privacy while overlooking atrocious ones. Protecting the Internet from cybercrime, terrorism, and other acts of sabotage is a multi-faceted problem with political, legal, technical, and social ramifications. Despite hyperbole surrounding efforts to reduce Internet abuses, it is not entirely clear what is at stake. What is the price of freedom? What are we willing to sacrifice for the sake of freedom? Outside of politics, these questions are not often asked directly, but are implicit in the security vs. freedom debate. Internet-facilitated political changes have been remarkable, but also give us pause. To what extent may the Internet be used to foster discontent and inflame tensions between Israelis and Palestinians or Iraqi Sunnis and Kurds? How may it be used to mobilize Chinese and Japanese citizens to go to war over a small group of disputed islands?

Impact of Anonymity in Business Transactions

Since its inception, the Internet has evolved from serving merely as an information repository to become a vibrant market and social-gathering place. While the Internet's role has changed and expanded, its basic structure has not. Efforts to integrate new roles into the same old model have not been completely successful. The economic Internet evolved spontaneously and the problems were only realized once commerce was already intricately embedded in its functioning. As we embark on an epic endeavor to recreate the electric grid across the world, using Internet technologies warrants a moment of pause to rethink the technology' basic paradigm. As we struggle to find the right

[3] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107
[4] http://daccess-ods.un.org/access.nsf/Get?Open&DS=S/RES/1368%20(2001)&Lang=E&Area=UNDOC

balance on the Internet between anonymity and security, we need to understand that it is not only a social medium, but also an engine that powers the world economy. The Internet has integrated international trade by providing the infrastructure to link goods, services, and resources across the world. As critical as this infrastructure is, it has been created piecemeal and is both unsecure and fragile. We continue to modify the current Internet to accommodate fast-changing needs, which adds burden to an already fragile system. I define the challenge faced in accommodating the competing objectives of freedom and security on the Internet in the subsequent subsection.

The Challenge

We need a resilient Internet that can accommodate new innovations while safeguarding fundamental values of freedom of speech and anonymity. We also need the same Internet to facilitate electronic commerce and support critical infrastructure. The balance between anonymity (that provides personal freedom) and its antithesis, traceability (that provides the ability to track and trace undesired activities), is shrouded in ambiguity that is not easy to resolve. If we are unable to reach a meaningful solution to this problem, the Internet in its current incarnation faces an existential threat wherein we will end up with multiple Internets where each Internet would be designed to have a different balance between privacy and traceability based on the specific role of the Internet. While this may solve the security vs. privacy dilemma for specific applications, it will create logistics challenges and seriously impact net neutrality tenets. Security and anonymity differ in importance based on the application in question: business applications require security and privacy, social networking applications require privacy and anonymity, and critical infrastructure communications require traceability to identify faults and other criminal activity. The first challenge is to be able to achieve both these objectives without seriously compromising on either.

I attempt to understand the business needs both from the previous evolution and from the potential for future innovation as I discuss this challenge. I start by using electronic commerce as a template (a situation where scientists and engineers have struggled to cobble together a system for consummating secure transactions in an insecure environment) and juxtapose that to the problem we face in the smart grid today. Privacy, in the context of electronic commerce, relates to ensuring that personal, private, or sensitive information is secured appropriately. It has parallels in the smart grid. Just like electricity usage data can reveal user behavior, purchases made through the Internet can reveal lifestyle choices. The ability to keep secure financial transactions has enabled businesses to move from brick-and-mortar stores to the digital marketplace. However, significant privacy breaches, such as those affecting AOL in 2006 and Sony's PlayStation® Network in 2011 and its film division in 2014, diminish trust in Internet transactions, and can lead to substantial negative impact on corporate profits (Goel & Shawky, 2009). The cost of security breaches in smart grid could be much more damaging than just financial losses. The second challenge is to recognize the current flaws of the Internet and fix them at a fundamental level rather than relying on a patchwork of short-term fixes done piecemeal. We not only need to design the smart grid to overcome existing flaws but to project into the future and design it in anticipation of future needs.

IV. POTENTIAL SOLUTIONS TO THE CHALLANGE

The communication infrastructure for the smart grid is being designed on the principles of the existing Internet, which has demonstrated security weaknesses. Basing the smart grid on the existing Internet model while postponing dealing with the security challenge is fraught with risk. It requires a priori reevaluation of the design and function of the Internet, starting from its genesis to its anticipated evolution. The smart grid meters will connect to servers to supply data on electricity usage, pricing, and grid operational characteristics without human intervention. The cardinal principle of anonymity needs to be questioned in context of the smart grid. Does a conversation between machines require anonymity? Meanwhile, traceability, the antithesis of anonymity, would not only help track hackers, but also dissuade users from committing fraud. Since traceability is already a feature of the existing power grid insofar as usage can be linked to specific households, why should it be any different when it is enabled through the Internet. We need to have a public debate on adding traceability into the Internet that is switched on only for industrial applications.

The Internet has a complex layered architecture, which results in vulnerabilities that are exploited for security breaches. For instance, the Internet's design is based on an addressing system that allocates an address to each node in the network. On top of the addressing system is the Doman Name System (DNS), which is a hierarchical distributed system for naming resources on the Internet and mapping them to addresses. The DNS translates text-based names (i.e., URLs) to numerical IP-addresses. A pointer from one URL can change from one IP-address to another transparently by simply updating DNS registries. The mnemonic, easy-to-remember names and the ability to change IP addresses is important in the current Internet for ease of use. However, DNS presents major vulnerabilities that have been exploited by multiple information security threats (e.g., cache poisoning, denial-of-service, flooding, etc.). For the smart grid network in which machines (smart meters, sensors, computers, etc.) are talking to each other rather than humans, do we really need a DNS? Do we really need to have separate MAC and IP-addressing schemes? Perhaps we can collapse the OSI / Internet stack into fewer layers.

The current Internet incorporates encryption on a piecemeal basis for different applications. End-to-end encryption could be instituted such that the vulnerabilities are only at the source and destination rather than through the entire channel. Should encryption be the default standard pervasive across the entire smart grid since all information needs to be secure? People fear that not only hackers and criminals will misuse information, but also that government, law enforcement, and utility companies will, too. These entities may have a legal right to access data. but we have to ensure through policies and regulations that there are strict control on how such data can be used, that there are proper legal underpinnings for government agencies, and that consumers' consent is obtained. There is already concern that foreign governments are clandestinely probing other countries' critical infrastructure to identify vulnerabilities to exploit. Often, such surveillance is done through spoofed identity and proxy entities. Can we design the smart grid network that minimizes if not eliminates the chances of spoofing? Given the vital importance of the power grid to any nation's security, it is essential that protocols used to maintain stability and security be incorporated into the smart grid's design from the ground up, rather than as an afterthought. A separate Internet, devoted solely to managing the electricity supply, will still have vulnerabilities as will be discovered during operations, but should be relatively more secure if the lessons learned from the Internet are used to guide its construction.

We not only have to design the smart grid based on current needs, but also based on possible future requirements. The present-day electric grid is power plant-centric; a majority of electricity is generated by a few large power plants that supply the grid. One of the smart grid's objectives is to facilitate energy generation; it is clear that, due to logistics issues, the current design has to change to obtain sufficient energy through alternate energy sources. We need to rely on the potential of millions of users with micro-generation capability (e.g., solar, wind) in individual households. It is not inconceivable that the power grid would become a market-driven open system that allows users to actively participate in controlling their usage. Thus, in the future, power may flow peer-to-peer rather than only from the utility to the consumer. This will create an energy web driven by market forces that allows users to auction and bid for electricity.

The smart grid will be dominated by machine-to-machine communication that will require traceability, not anonymity. We will need complete traceability not only to minimize chances of market fraud but also to dissuade perpetrators of critical infrastructure intrusions from launching attacks. International treaties to reduce chances of cyber warfare are currently stymied because of lack of attribution—again a consequence of anonymity. No matter how we look at it, anonymity is an untenable concept for the new smart grid, and its architecture needs to reflect this for a safer and more-secure grid. There are efforts to tackle security and privacy issues by the international bodies as I discuss below, but much work needs to be done that may lead to radical changes to the Internet. To reduce the probability of detailed metering data from households revealing consumers' lifestyles and behavior, new approaches need to be developed such as temporal data aggregation for billing purposes and spatial data aggregation for forecasting or adding noise to data to prevent it from revealing personal user information (Khurana, Hadley, Ning, & Frincke, 2010; Efthymiou & Kalogridis, 2010).

Not only do we need to protect consumers through technical means, but we need to follow this up with legal means. There has been a concerted effort across the United States and the European Union to develop standards and guidelines to protect consumer data. I discuss some relevant standards and legislations in the next subsection.

Laws and Standards Relevant to Smart Grid Privacy and Security

The smart grid uses fine-grained usage data for operational needs such as load forecasting, demand response, and load balancing, and smart meters form the first point in the collection and transmission of smart meter data. This data allows utility companies to gain visibility into the grid for better monitoring and control and, at the same time, inform users about their own usage patterns for making smart energy choices. This information is very potent and can reveal lifestyle choices and behaviors of users that can be exploited for several purposes including discrimination, marketing, and litigation. For instance, electricity usage data can be used to detect marijuana growing operations in homes quite reliably, and police routinely issue subpoenas for obtaining electricity usage records of suspected growers from utility companies. The regulators' goal is to ensure that the data are adequately protected from interested entities such as hackers, rogue businesses, intelligence organizations, and law enforcement.

Given the wireless transmission of data from smart meters, law enforcement will be able to just tap into the wireless network and obtain the data without requiring legal authorization. Whether or not users are protected from law enforcement to tap into smart meters without the need for subpoenas is unclear. The fourth amendment to the constitution of the United States guarantees the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures (U.S. Const. am. 4). The fourth amendment specifically bars search and seizure without probable cause and legal authorization. Based on the fourth amendment law, enforcement should not be able to tap into the smart meter to obtain metering data for an individual; however, this has not been tested in courts for smart meters, which creates ambiguity. There has been a public debate on whether

gathering such data is a violation of the fourth amendment of the constitution. For instance, there is a recent court case regarding Apple's Touch ID feature (i.e., one can use their fingerprint as a passcode on newer models of the iPhone and iPad). Law enforcement is not legally permitted to ask the user to disclose their passcode to unlock their phone since it violates the fifth amendment; however, they can ask the user to use their finger print to unlock the device, which ostensibly does not violate the fifth amendment. Clear guidelines for using smart data by law enforcement need to be established to protect smart meter adopters from such ambiguities.

The Electronic Communication Privacy Act (ECPA) acts against interception of electronic communication and protects citizens from government surveillance; however, it does allow government to conduct surveillance on private communication between two parties if one of the parties provides consent to such surveillance. The transmission of smart meter usage data from consumer to utility company falls under the preview of ECPA, which implies that a utility company's consent would be sufficient to launch government surveillance. This is an obvious intrusion into households and raises concerns about collusion between utility companies and government and needs public debate. Similarly, the Stored Communications Act (SCA) would protect users from illegal access to stored metering data. It limits third party organizations from collecting personal data to disclose data to other parties. The data may be stored in database servers of the utility company or on the smart meters themselves, which would fall under the preview of this legislation. The Computer Fraud and Abuse Act prohibits unauthorized access of computerized information used in interstate commerce, which would cover smart meter data because it is used for commerce. These statutes, however, will permit law enforcement access to smart meter data for investigative purposes based on just cause and with legal authorization. We need to ensure the same protections for smart meter data. A further debate is whether smart meter data are more intrusive that would require additional protection.

Consumers expect utility companies and third-party smart grid providers to follow standard privacy and information security practices to protect user privacy; however, the concern is that some of the parties may not be completely trustworthy. Worse still, the utility companies may sell consumer electricity usage data to third parties for financial gain. There are provisions for telephone data that can be used as a starting point for defining similar provisions for smart grid data. Privacy experts also need to develop privacy preserving schemes in data sharing across multiple organizations, which may include aggregating temporal and spatial data aggregation, anonymization of metering data, data obfuscation, and cryptographic protocols.

Several standards and guidelines are emerging to address the issues of smart grid privacy both in the United States and the European Union. NIST (2013) classifies smart grid data into two categories: type I and type II. Type I information did not exist before and is specific to the smart grid. Type II information existed before and is also available from the smart grid. They contend that type II information will most likely be covered by existing privacy legislation in other fields; however, for Type I (such as using fingerprints as a passcode for iPhones or iPads) information, new safeguards are needed. NIST makes several recommendations that include: assessing privacy prior to adoption of smart meters, establishing privacy policies and procedures inspired by Organization for Economic Co-operation and Development (OECD) principles, developing privacy-use cases, educating the public about privacy risk, and constraining data collection based on actual need. The Department of Energy has released its own set of voluntary privacy recommendations for smart grid owners, operators, and third parties (DOE, 2012). The recommendations cover several issues that include measures that utility companies should take to inform consumers about their privacy rights, justification for data collection (i.e., what data are being collected, how it is being collected, why it is being collected, and how it will be used), rules for data sharing, consumer consent (including ability to opt-in and opt-out), and consumer access to their own data.

The European Commission is currently reviewing the European Union's legal framework for the protection of personal data to not only modernize the existing framework but also to meet the challenges that globalization and the evolution of technology pose. The commission wants to strengthen individual rights without attenuating the free flow of information and provide clarity and coherence to the rules such that they can be applied consistently. The commission has provided specific guidance to member states on protecting smart meter data through Directive 95/46/EC. In accordance with the directive, the commission has developed a data-protection template for protecting individuals' personal data that will assess the risks posed to the information. They recommend that the network operators and utility companies that manage the smart meters should adopt a risk-based approach and put technical and organizational measures in place to protect the data. A risk-based approach is a good start; however, it lacks the detail and comprehensiveness that is necessary for ensuring compliance with consistency. First, it does not adequately distinguish between threats and vulnerabilities and, second, it does not relate specific controls to different threats, but rather provides a catalog of threats and controls without any specific mapping. It also does not have a way of prioritizing threats by their relative impact. There is also much work to be done in identifying all the risks, let alone creating guidelines and treaties.

V. CONCLUSION

This discussion of the smart grid highlights the fact that, as the Internet has evolved, so has our understanding of the fundamental assumptions on which it is based. The different applications on the current Internet have varying fundamental requirements, and it may be time to contemplate the creation of multiple Internets with different sets of rules and assumptions. In order to achieve greater efficiency and reliability in the electricity grid and allow a bi-directional flow of power, our power infrastructure will be transformed by superposing a layer for communication infrastructure on the electric grid. This communication infrastructure will not only improve efficiency and provide network resilience but, can be leveraged to create an energy Internet where consumers directly buy and sell power to other users in the network. It is easy to replicate the protocols of the current Internet to create the smart grid network. The smart grid does not, however, have to be constructed on the same basis as the current Internet. It can operate with a different set of standards than those used to regulate electronic commerce and social networking. Rethinking the infrastructure design and basic assumptions that govern various applications would be a logical next step. If we are able to disentangle the fundamental requirements of these separate, potential Internets, we might even be able to construct systems that ensure greater security, but do not demand sacrifice of freedoms. The security vs. anonymity debate has, in the past, been a domestic issue to the United States, but it now has international connotations. Different countries have various policies on Internet policing that derive from specific laws, customs, and norms. The fact that the Internet transcends borders implies that conflicts affected by it cannot easily be resolved by laws drafted by individual nations. We cannot afford to have different rules for the Internet for different countries in order to able to support global integration in areas such as energy. As we contemplate the creation of multiple Internets and attempt to strike a balance between anonymity and security, we need to take differing perceptions of security and anonymity contextualized in social and political manifestations of society and streamline the process of building international consensus.

ACKNOWLEDGEMENTS

I thank Damira Pon, Anthony Belardo, Ethan Sprissler, and Ersin Dincelli for their editing, reviewing, and valuable suggestions to this paper. I also thank the anonymous associate editor in helping restructure the paper to make it suitable for the journal.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy? In A. Aquisti, S. Gritzalis, S. Di Vimercati, & C. Lambrinoudakis (Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 363-377). Boca Raton, FL: Auerbach Publications.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday, 13*(3). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/2142/1949/

Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. *Information Management & Computer Security, 11*(5), 209-215.

Axford, B. (2011). Talk about a revolution: Social media and the MENA uprisings. *Globalizations*, *8*(5), 681-686.

Berners-Lee, T. (2010). Long live the Web: A call for continued open standards and neutrality. *Scientific American Magazine.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html

Bonneau, J., & Preibusch S. (2010). The privacy jungle: On the market for data protection in social networks. *Economics of Information Security and Privacy*, 121-167.

Comunello, F., & Anzera, G. (2012). Will the revolution be tweeted? A conceptual framework for understanding the social media and the Arab Spring. *Islam and Christian–Muslim Relations*, *23*(4), 453-470.

Cranor, L. F. (1999). Internet privacy. *Communications of the ACM, 42*(2), 28-38.

DOE. (2012). *U.S. Department of Energy Smart Grid Privacy Workshop Summary Report*. Retrieved from https://www.smartgrid.gov/sites/default/files/doc/files/Privacy%20report%202012_03_19%20Final.pdf

Efthymiou, C., & Kalogridis, G. (2010). Smart grid privacy via Anonymization of smart metering data. *Proceedings of the 1st IEEE International Conference in Smart Grid Communications,* 238-243.

Eltantawy, N., & Wiest, J. B. (2011). Social media in the Egyptian revolution: Reconsidering resource mobilization theory. *International Journal of Communication*, *5*, 1207-1224.

Goel, S., & Shawky, H. (2009). Estimating the impact of security breaches on stock valuations of firms. *Information & Management*, *46*(7), 404-410.

Goel, S., Bush S. F., & Bakken, D. E. (Eds.). (2013). *IEEE vision for smart grid communications: 2030 and beyond*. IEEE Press.

Khurana, H., Hadley, M., Ning, L., & Frincke, D. A. (2010). Smart-grid Security Issues. *IEEE Security & Privacy, 8*(1), 81-85.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (1997). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22-31.

Lessig, L., & McChesney. R. W. (2006). No tolls on the Internet. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html

NIST. (2013). *Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high level requirements*. Retrieved from http://csrc.nist.gov/publications/drafts/nistir-7628-r1/draft_nistir_7628_r1_vol1.pdf

Tufekci, Z. (2011). New media and the people-powered uprisings. *MIT Technology Review*. Retrieved from http://www.technologyreview.com/view/425280/new-media-and-the-people-powered-uprisings/

Verzi, D., & Coates, B. (2004). Balancing freedom & security in the Patriot Act 2001: A mathematical model. *Journal of Interdisciplinary Mathematics*, *7*(1), 29-39.

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, 2, 141-176.

ABOUT THE AUTHOR

Sanjay Goel is an Associate Professor and Chair of the Information Technology Management Department in the School of Business, and the Director of the Forensics Analytics Complexity Energy Transportation and Security (FACETS) Center at the University at Albany, State University of New York. He received his PhD in Mechanical Engineering from Rensselaer Polytechnic Institute. He previously worked as a researcher at the General Electric Global Research (GE). His research interests include information security, privacy, cyber warfare and cyber physical system (Smart Grid and Transportations) security, media piracy, self-organization, and engineering optimization. He has done extensive work on aircraft engine and power turbines at GE. He won the promising Inventor's Award from the SUNY Research Foundation in 2005, SUNY Chancellor's Award for Excellence in Teaching in 2006, UAlbany Excellence in Teaching Award in 2006, and the UAlbany Excellence in Research Award in 2010. He was named one of the three AT&T Industrial Ecology Faculty Fellows for 2009-2010. He has received grant funding from multiple sources including: NIJ, U.S. DOE, NSF, NYSERDA, and James S. McDonnell Foundation. He has published in several leading journals including *California Management Review, IEEE Journal of Selected Areas in Communication, Decision Support Systems, Communications of the AIS, Journal of Strategic Information Systems, Communications of the ACM, and Information & Management Journal.*

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems