neustar

NEUSTAR WHITE PAPER:

WHEN SMART GRIDS GROW SMART ENOUGH TO SOLVE CRIMES

March 18, 2010

I. INTRODUCTION

Telecommunications carriers and Internet service providers enjoy a close-up view of our lives. They see our telephone calling patterns, track our mobile whereabouts, store our emails, and memorize our Internet browsing habits. No wonder these communication service providers often get caught in debates about the privacy of communication activities.

Privacy-minded subscribers expect communication service providers to keep subscriber activities confidential. Law enforcement expects to view certain activities promptly upon request. If the service provider under-discloses or over-discloses information to law enforcement it risks legal liability.

As a result, a large and complex set of statutes, regulations, and court rulings has evolved to address these sensitivities. These sometimes confusing pronouncements have impacted non-communication industries as well.

Will a similar wave of privacy and disclosure laws engulf the utility industry? As electricity, water, and gas utilities deploy smart grid systems, they too will have access to data that will potentially reveal personal aspects of our lives. Utilities that have implemented smart grids may not know who we communicate with, but they might infer that we are watching a plasma screen HDTV, cooking dinner, or working on a computer. They could potentially notice the temperature we keep our homes, how often we take showers, and when we turn off our bedroom lights.

This white paper will summarize the legal relationship between privacy and criminal due process, primarily in the communication industry. It will then explain why a similar regulatory structure may be needed for smart grid deployments. A "smart grid" is assumed to be any network deployed by a utility that includes two-way digital technology to control the transmission or distribution of electricity. Hopefully, the discussion will help utilities prepare for the potential policy clash between ratepayer privacy and law enforcement.

II. COMMUNICATION SERVICE PROVIDERS MUST PROTECT SUBSCRIBER PRIVACY BUT STILL DISCLOSE CERTAIN SUBSCRIBER ACTIVITIES TO LAW ENFORCEMENT

In the early 20th Century, when the first telephone networks were deployed, few people considered the need to protect the privacy of these electronic communications. Perhaps even fewer realized how vital the networks could be to the mission of law enforcement. At the time, a phone call was viewed simply as a way to converse across great distances.

A. The Advent of Lawful Electronic Surveillance

Telephone company engineers traditionally tested the signal quality of their networks by listening to samples of customer conversations. Law enforcement agencies ("LEAs") then used similar listening devices as a safe and efficient way to investigate criminal suspects. The resulting recordings made for reliable evidence in court. Today, the techniques of lawful electronic surveillance are used to foil terrorist plots, penetrate illegal drug rings, and solve other serious crimes.

B. The Use of Billing Records to Track Criminal Suspects

LEAs also learned the value of subscriber billing records. These are the monthly statements that document the telephone numbers a subscriber dialed and the numbers assigned to those who called the subscriber. The records include the date, time, and duration of the inbound and outbound calls.

Today, law enforcement analysts apply sophisticated algorithms to the patterns of these ordinary records to make far-reaching statistical predictions about criminal organizations. The analysts can determine with remarkable accuracy which telephone number belongs to the ring leader, which belongs to an associate, who operates in the inner circle and who dabbles on the periphery, when the group is planning a crime, and when the crime is imminent.

C. The Need to Protect Communication Privacy

Eventually, the recording of voice conversations and sifting of phone records became attractive to interests other than law enforcement. Pranksters, politicos, and marketing firms all learned to exploit these informational resources for their own disparate ends.

As communications technology grew more sophisticated, it took more imprints of our lives. For example, cellular radio engineers developed a way to identify a person's geographic location. Email put more thoughts in writing. IP login records revealed not only who contacted whom on what dates and times, but also the types of text, videos, and music they accessed on the Internet. With each innovation came renewed cries for privacy.

D. The Legal Arrangement to Protect Communication Privacy and Assist Law Enforcement

In the U.S., the regulatory approach to electronic communication privacy imposes a general prohibition against the disclosure of subscriber information but permits various complex exceptions to the ban as needed for legitimate purposes such as law enforcement. The following summarizes the required standards of review and capabilities.

1. Required Standards of Review

The more private the information, the higher the legal hurdle that law enforcement must clear to obtain communications network information in a criminal proceeding. For example, an LEA may readily obtain a suspect's billing records as long as they are "relevant" to an ongoing criminal investigation. Where an LEA believes the relevance standard is met, it may unilaterally issue a subpoena, serve it on the communications carrier, and thereby compel the carrier to disclose the targeted records. By comparison, if the LEA needs to read a suspect's emails or intercept his voice communications, it must meet a higher level of suspicion, called "probable cause," and submit the showing to a judge. Only if the judge finds the showing sufficient will he or she issue a search warrant or a court order authorizing the investigative action.

2. Required Capabilities

Service providers are not directly required to conduct surveillance on suspects for law enforcement. However, they are expected to build technical capabilities into their networks that can isolate, duplicate, and re-route a suspect's communications to a law enforcement surveillance point in real-time when surveillance is ordered by a court. The whole process must be undetectable by the suspect and cause no more than minimal interference with the communication service. Depending on the terms of the court order, the carrier may need to filter and transmit just the call-identifying information without sending the audio portion of the call. Time and date stamps are also required to help LEAs track the communications.

As for subscriber records, the general rule is that a carrier must give law enforcement only those records for a given suspect that the carrier produces in the normal course of business. Those records must often be redacted to remain within the scope of the given subpoena. For example, if the subpoena requires three months of the suspect's "outbound" calling records, the carrier must delete the inbound calling records from the three-month group of bills.

Communication providers must also retain telephone billing records for 18 months in case they are needed by law enforcement. A pending Federal Communications Commission proceeding may additionally require carriers to destroy the data after a certain deadline so it is no longer vulnerable to unauthorized access.

E. The Compliance Burdens on Communication Service Providers

The U.S. privacy laws are administered by Congress, the FCC, the Federal Trade Commission, the states, and the courts. Multiple privacy groups watchdog the communication industry and participate in public proceedings. The laws evolve continuously as new privacy issues arise.

To cope with these burgeoning demands, service providers must adopt formal compliance policies and procedures. The larger providers maintain dedicated staffs to manage the law enforcement assistance burden. In a typical year a large carrier may receive hundreds of court orders mandating lawful intercepts and hundreds of thousands of subpoenas for billing records. If the carrier over-discloses information by providing details beyond those requested in the subpoena, it could provoke a subscriber privacy complaint. An under-disclosure of items demanded by a subpoena could trigger court sanctions. In some situations, a failure to assist law enforcement could literally let a criminal get away with murder.

III. OTHER INDUSTRIES MUST ALSO PROTECT PRIVACY AND ASSIST LAW ENFORCEMENT

Communication service providers are not the only businesses subject to law enforcement inquiries. Airlines, credit card companies, hotels, banks, and rental car companies all receive subpoenas seeking records on criminal suspects. Consequently, these entities have procedures to protect the privacy of their records and respond to the law enforcement requests.

IV. SMART GRIDS MAY BECOME SUBJECT TO INCREASED PRIVACY AND DISCLOSURE DEMANDS

Just as the public a century ago could not imagine the need for privacy protection in telecommunications, people today may overlook the need for such safeguards in utility services. After all, utilities do not currently glean many details about our lives. They essentially take monthly readings of electricity, water, and gas usage, and generate monthly bills. However, that standard business practice is rapidly changing.

A. More Frequent Meter Readings Tell More About Consumers

Utilities have found that they can supply energy more efficiently, and let consumers draw energy more efficiently, by deploying IT applications that monitor the usage more closely. These intelligent systems achieve the improved monitoring through the use of smart meters. Like traditional electric meters, a smart meter is installed on the premises of a home, office or other building to measure the occupant's energy use. Unlike traditional meters, a smart meter can take usage readings more frequently than once a month. Some smart meters already sample usage as often as every 15 minutes, and future versions of the device may take snapshots every six-to-eight seconds or in real time. Thus, usage patterns can be increasingly monitored in granular detail. (For a fuller description of smart grid capabilities, see "Smart Metering & Privacy:

Existing Law and Competing Policies, a Report for the Colorado Public Utility Commission," by Elias Leake Quinn, Spring, 2009).

A smart meter alone cannot tell whether you cook dinner with a microwave oven or a stove. However, industry experts expect that in several years household appliances could be fitted with ID chips that permit such device-specific monitoring. Assuming utilities retain their smart meter readings, they could analyze the records to make valuable inferences about energy usage trends. The energy providers may retain the records in-house or with third-party firms. The length of data retention could be temporary, permanent, or something in between.

B. Law Enforcement Already Investigates Certain Existing Utility Records

In at least one respect, utility information has already proven valuable to law enforcement. LEAs have occasionally examined electric bills in drug investigations. For example, unusually high volumes of electric consumption at the residences of suspected drug dealers are sometimes linked to "grow lights," which are used in marijuana-growing operations. Electric companies typically disclose these exorbitant bills to LEAs under the same legal process used for the disclosure of communication subscriber records: the LEA issues a subpoena for the bills under the relevance standard, and the utility delivers the requested records.

The question remains, what type of information could law enforcement possibly want from smart grids? Potentially, plenty. The following speculates on the possibilities.

C. Law Enforcement Investigations May Increasingly Involve Smart Grids

Law enforcement may need smart grid data to assist three types of investigations: regular crime; cyber crime; and threats to the smart grid itself.

1. Regular Crime

A smart grid could help law enforcement determine whether a building is used for a criminal operation. In the above example of the marijuana grower, analytic software might have inferred from the suspect's usage pattern not only that he was consuming an unusual amount of electricity but that the consumption was consistent with a grow light operation. Such higher-quality evidence could improve the LEA's chances of persuading a judge to sign a search warrant permitting agents to enter and search the house. Similar types of smart grid pattern analyses might help identify a sweat shop, brothel, illicit distillery, or a business used as a front for criminal activity such as money laundering.

Sometimes an LEA is less concerned about the use of a building than the conditions prevailing at the scene of a crime. For example, smart meter readings that record the instant of a power outage may mark the detonation time of a nearby car bomb. A sudden surge in air conditioning may pinpoint the moment when a burglar broke through a glass door or window. A long absence of running showers or baths in the home of a suspected child abuser may contribute to evidence

of the abuse. Finally, the operation of video equipment and klieg lights in the home of a suspected producer of child pornography may also be incriminating.

Energy records may also reveal a suspect's location at the time of an offense. He may have been recharging his electric car near his office, opening the garage door at his home, or using an electric blanket in his bedroom. If there is an outstanding warrant for his arrest, authorities would need to know his location right now. That is where real-time smart meter monitoring could prove valuable.

Finally, smart meter analysis could help enforce state and local ordinances. Maybe a landlord has violated the housing code by keeping an apartment building insufficiently heated in the winter. A business may have used industrial machinery on property zoned for residential use. A homeowner may have illegally rented out a basement. Or a ratepayer may have wasted water during a period of water rationing.

2. Cyber Crime

To the extent that smart grids let customers control their own energy use through IT commands, utilities will need to develop systems of "identity management" similar to those used in ISP networks, where subscribers establish user names and passwords. The risk of identity management systems is that they are vulnerable to cyber crime. For example, criminals might use a homeowner's virtual identity to "steal" energy. Alternatively, they could commit burglaries at times when energy readings show the victims are not home.

Cyber crime is nothing new to law enforcement. They have teams of experts dedicated to combating these computer crimes. For example, when a criminal launches a "phishing attack" by duplicating the web site of a bank to obtain depositor information, law enforcement agents and IT engineers try to trace the scam back to its source. Their success depends in part on industry cooperation. Accordingly, law enforcement will likely need the assistance of utilities to investigate any cyber crime that spreads to smart grids.

3. Threats to the Smart Grid Itself

Perhaps the greatest fear of any smart grid architect is that the utility's IT infrastructure will be damaged by a natural disaster or terrorist attack. A consulting firm specializing in cyber-security recently published a report stating that certain non-U.S. actors are almost certainly targeting and penetrating the networks of U.S. energy providers. *See* "Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and emerging Threats," January 21, 2010, http://www.scribd.com/doc/25550091/Proj-Grey-Goose-report-on-Critical-Infrastructure-Attacks-Actors-and-Emerging-Threats.

These risks are major concerns of law enforcement. In fact, the nation's homeland security strategy, developed after the 9/11 attacks, gives law enforcement a leadership position in

defending against cyber attacks and an equally important role in guarding "critical infrastructure" such as electric utilities. Utilities should therefore expect more demands from law enforcement on these matters.

D. Retailers and Civil Litigants May Also Seek Access to Smart Grid Data

LEAs are not the only ones with an interest in accessing smart grid data. Retailers of consumer durables would presumably want to know who buys which brands of toaster ovens, dishwashers, washing machines, and other appliances, how often the devices are used, and for what durations. Perhaps any utility-related consumer behavior would be valuable to some marketing initiative. Some ratepayers may be willing to disclose their behavior patterns but others are bound to refuse. In any event, the potential for commercial exploitation of smart grid data reinforces the need for smart grid privacy.

Privacy threats could also arise from civil litigants. A party to a divorce proceeding may serve a subpoena on a utility to obtain smart meter records on an ex-spouse's whereabouts or lifestyle. Civil litigation demands already flood the records production departments of communication service providers. It stands to reason that these legal instruments will also inundate utilities.

V. THE PRIVACY/DISCLOSURE MODEL STRUCTURED FOR COMMUNICATION SERVICES COULD BE APPLIED TO SMART GRIDS

The communications industry is perhaps the best model to study when forming policies for smart grid privacy and disclosure. Just as communications providers monitor and retain a rich variety of information about their subscribers, with different types of data requiring different techniques of disclosure and different levels of privacy protection, so will smart grids create the ability to track and store a variety of data that will likely require a multi-tiered approach. The smart grid is essentially the addition of a communications network to the current energy distribution grid. Once a communication network is overlaid on a utility network, energy consumers and businesses will probably want both layers of operation to be subject to a common set of laws.

The most basic principle of electronic communication privacy is translatable to the utility industry. Specifically, all consumer data is presumptively private until and unless a party who seeks that data qualifies for one of the statutory exceptions. In the utility context, like the communication context, appropriate exceptions could be granted to law enforcement and perhaps others.

Beyond this basic principle, the following shows how the privacy/disclosure model of the communication industry could be applied to smart grids.

A. Potential Standards of Review

Just as some types of communication data are given more privacy protection than others, the same will probably be true of smart grid usage data. Statutes may mandate that the more

sensitive elements of utility data must be disclosed to law enforcement under the above-described probable cause standard, while the more ordinary ones are disclosed under the lower relevance standard. Various factors have been used by legislatures and the courts to define what data is sensitive: whether the data reveals an intimate detail about a person's life; whether it is readily observable through other means; and whether it is knowingly disclosed by the consumer to the service provider.

B. Potential Capabilities

As noted above, communication service providers must build certain technical capabilities into their networks to serve the needs of law enforcement. Similar requirements may be applied to the IT infrastructure of utilities to assist the kind of criminal investigations described above.

As also explained, when a communication provider receives a valid subpoena, it must disclose any relevant records kept in the normal course of business and perform any needed redaction of information not covered by the subpoena request. Further, the service provider must retain the data long enough for law enforcement to use but may be required to destroy the data after a mandated period. Utilities may likewise be required to disclose records kept in the normal course of business. They may also become subject to mandates of retention and destruction.

C. Other Considerations

When a party serves a communication provider with a subpoena for subscriber records, the provider may be required to notify the subscriber. That way the subscriber has the opportunity to challenge the subpoena, for example with a motion to quash. In other cases, the subpoena may require the carrier not to notify the subscriber. Such a 'do not disclose' order may be needed to avoid tipping off the subscriber to a criminal investigation. In the context of a subpoena for smart grid usage records, there could be a similar mix of situations where notices to ratepayers are required or prohibited.

As long as a communication provider handles a subpoena properly, it is shielded by "statutory immunity" from lawsuits for any resulting damages to other parties. Smart grid utilities could be given a similar legal protection.

VI. SMART GRID UTILTIES COULD LEVERAGE THE COMMUNICATION INDUSTRY MODEL TO PREPARE FOR THE LIKELY RISE OF SMART GRID PRIVACY AND DISCLOSURE DEMANDS

Because the communication industry model for privacy and disclosure is such a natural fit for the utility industry, smart grid-enabled utilities could leverage that model to their advantage. The following reviews the steps they might take.

A. Incorporate Privacy and Disclosure Capabilities at the Design Stage

Utilities, like communication network owners, could design their smart grids with the needs of privacy and law enforcement in mind. For example, they could design technical capabilities enabling law enforcement to conduct real-time lawful surveillance of energy events. In addition, they could install automated systems to store, retrieve, redact, and transmit smart meter records kept in the normal course of business.

B. Develop a Compliance Program

Next, smart grid utilities might follow the example of communication carriers by establishing privacy/disclosure compliance programs. The programs might permit only certain authorized and trained employees to respond to law enforcement requests. These employees would serve as points of contact to law enforcement, review the court orders and subpoenas served on the utility, challenge those that are legally defective, and process the valid ones by the applicable deadlines. They might also provide privacy and disclosure training to internal groups such as network engineers and customer care staffs. Finally, they might draft ratepayer documentation, including privacy policies and related public relations materials, to limit contractual liability.

The compliance program might include security measures. In particular, smart grid data could be protected with encrypted storage, password protection, and authorized rights of access, with policies for data retention and destruction. Adopting a formal retention policy could help avoid disputes with law enforcement, such as where an LEA requests 18 months of usage data from a utility that retains the data for only 12 months.

C. Establish Industry Best Practices

Also advisable is an initiative to establish industry-wide practices for the handling of smart grid data. These practices would help manage LEA expectations and develop safe harbor standards to minimize risk. For example, industry may collectively determine that some data elements can be feasibly disclosed in real time while others must remain available only as historic records. Already, industry and government have taken an admirable first step in the direction of best practices by holding a public proceeding to examine the issues of smart grid cyber security and privacy. See "Draft NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements," http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf.

D. Participate in the Law Making

Finally, smart grid developers may want to participate actively in the development of any laws or regulations governing the privacy and disclosure of smart meter data. These laws or regulations could be introduced by Congress, state legislatures, or public utility commissions. In each forum, the utility industry will likely find useful precedents in the communication industry.

VII. CONCLUSION

For many industries that collect and store customer data, the task of managing data privacy and disclosure is a cost of doing business. Until now, utilities have been affected only lightly by this trend.

However, as utilities migrate to smart grid systems, the types of data they collect will become more valuable to law enforcement and other interests. These informational treasures will probably create policy disputes. Many voices in the debate will likely be those of the ratepayers, many of whom will no doubt insist that their personal information be kept private. Opposing arguments will presumably arise from law enforcement, based on its need to access the same data to investigate crimes.

These regulatory quarrels may put utilities in a bind. The entities may welcome the intervention of law enforcement for purposes of responding to natural disasters, as well as defending against cyber attacks and cyber crime, but resist the burdens of other LEA tasks, such as regular criminal investigations. One thing is certain: when law enforcement comes knocking on the utility company's door, the utility cannot lawfully say, 'Sorry, we're not ready.'

Utilities should anticipate the predicted conflicts over privacy and disclosure. In particular, they should consider following example of communications service providers by designing networks, assembling compliance programs, and taking related steps to meet both policy goals.

It may take years for the smart grid industry to strike a fair balance between privacy and law enforcement. But the effort is advisable. Utilities do not want to be put in a position where they may anger customers, violate judicial orders, or potentially cause public safety harm.

Should readers have any comments on this white paper, please direct them to Joel M. Margolis at *joel.margolis@neustar.biz*.

About Neustar

Neustar, Inc. (NYSE:NSR) solves complex communications challenges and provides market-leading, innovative solutions and directory services that enable trusted communications across networks, applications, and enterprises around the world. Neustar Legal Compliance provides telecommunications carriers and Internet Service Providers with the technical solutions and compliance programs they need to meet their law enforcement assistance obligations. Visit Neustar online at www.neustar.biz.

About Joel M. Margolis

Joel M. Margolis is the Senior Director of Neustar Legal Compliance. His 26 years of telecommunications law practice includes lengthy backgrounds in both the communications industry and government. He served as Senior Regulatory Counsel of Nextel Communications,

Inc., where he specialized in federal regulations governing E911 emergency calling, lawful electronic surveillance, and subscriber privacy. He later worked as the Assistant Deputy Chief Counsel of the Drug Enforcement Administration. There he represented the agency on certain Department of Justice working groups assigned to update federal legislation governing lawful surveillance, communications subscriber privacy, and related matters. He is frequently a panelist at industry conferences where the above issues are explored.