Nova Law Review

Volume 36, *Issue* 3 2012 *Article* 5

A Look at the Proposed Electronic Communications Privacy Act Amendments Act of 2011: Where is Smart Grid Technology, and How Does Inevitable Discovery Apply?

Darlene Bedley*

*

Copyright ©2012 by the authors. *Nova Law Review* is produced by The Berkeley Electronic Press (bepress). https://nsuworks.nova.edu/nlr

A LOOK AT THE PROPOSED ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS ACT OF 2011: WHERE IS SMART GRID TECHNOLOGY, AND HOW DOES INEVITABLE DISCOVERY APPLY?

DARLENE BEDLEY*

* Darlene Bedley is a J.D. Candidate, May 2013, Nova Southeastern University, Shepard Broad Law Center. Darlene received her Bachelor of Science in Ceramic Engineering, and her Masters in Business Administration with a Marketing Concentration from Rutgers University. The author is a registered agent to practice before the United States Patent and Trademark Office in patent cases. The author wishes to thank her fiancé for his love and encouragement, her wonderful daughters for believing in their mom, her future step sons for being thoughtful during study time, and her family for their support and encouragement. The author wishes to extend sincere gratitude to Associate Dean Catherine Arcabascio for her advice and guidance. The author would also like to thank the members of *Nova Law Review* for their hard work, with a special thanks to Jaime Weisser for her dedication to the training program.

I. INTRODUCTION

Cloud computing and smart grid technologies increase efficiency and lower costs to telecommunication and energy consumers.[1] In addition, smart grid technology results in lower fossil fuel consumption, and is therefore considered a green technology.[2] U.S. privacy law has not kept up with the pace of these technologies, especially in the area of Fourth Amendment protection.[3] Specifically, search warrants are not required for government access of information remotely stored by third party providers in some cases.[4] This area, known in the industry as digital due process, requires reformation to the existing Electronic Communications Privacy Act of 1986 (ECPA).[5]

Currently, there is proposed legislation on this topic, which was introduced to the Senate on May 17, 2011 as the Electronic Communications Privacy Act Amendments Act of 2011.[6] The proposed legislation includes an updated requirement for a search warrant for government access of information remotely stored by third party providers and addresses some of the Fourth Amendment protection issues.[7]

This paper will suggest that the proposed legislation should include smart grid technology. In addition, this paper will suggest that the independent source doctrine and the inevitable discovery rule should be considered because they may undermine the proposed legislation's goals. The next sec-

1. *Energy Bar Association Panel Discussing the Smart Grid*, 31 ENERGY L.J. 81, 85–86 (2010); Jitendra Pal Thethi, *Realizing the Value Proposition of Cloud Computing: CIO's Enterprise IT Strategy for Cloud*, INFOSYS, 2 (2009), *available at* http://www.infosys.com/cloud/resource-center/documents/realizing-value-proposition.pdf.

2. *Energy Bar Association Panel Discussing the Smart Grid*, *supra* note 1, at 89.

3. Nate Anderson, *Bringing US Privacy Law into the Cloud Computing Era*, ARS TECHNICA (Mar. 30, 2010, 5:55 PM), http://arstechnica.com/tech-policy/news/2010/03/bringing-us-privacy-law-into-the-cloud-computing-era.ars.

4. Electronic Communications Privacy Act, 18 U.S.C. § 2703(a)–(b)(1) (2006 & Supp. III 2009); Anderson, *supra* note 3.

5. Anderson, *supra* note 3; *see* Electronic Communications Privacy Act § 2703(a)–(b)(1).

6. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. §§ 1–3 (2011).

7. *Id.* § 3.

tion of this paper includes a brief and simplified overview of cloud computing and smart grid technologies. Economic and environmental benefits of both technologies are introduced in this section. Projections and statistics are included to provide a perspective of the potential reach of the proposed legislation.

The third section of this paper focuses on the current legal standards regarding privacy issues of cloud computing and smart grid technologies. Constitutional requirements under the Fourth Amendment are discussed. The outdated provisions of the ECPA are also outlined. This section contains an overview of *Katz v. United States*[8] and the current reasonable expectation of privacy standard. Further, the evasion of the electronic communications privacy issue by the Supreme Court of the United States in *City of Ontario v. Quon*[9] is presented. Following the *Quon* overview, this section addresses the third party exception doctrine. Finally, this section ends with a discussion of what would be a reasonable expectation of privacy in the cloud.

The fourth section will provide information on the proposed legislation that was presented to the Senate on May 17, 2011, which focuses on updating the ECPA and requiring the government to obtain a search warrant for access to information stored by third parties beyond the existing 180-day window.[10] This section recommends that because the energy companies will face similar issues as smart grid technology becomes universally available, smart grid technology should be included in the proposed legislation. Additionally, some exceptions that may challenge the goals of this bill are addressed in this section. Specifically, the independent source doctrine and the inevitable discovery rule may provide a circular way around the legislation. This section will explain both doctrines, and will suggest how these exceptions may provide loopholes that undermine the current proposed legislation's purpose.

The paper concludes with the Obama administration's position on the changes in the proposed legislation and recaps the economic benefits of the technologies. The conclusion summarizes the views presented in the third section.

8. 389 U.S. 347 (1967).

9. 130 S. Ct. 2619 (2010).

10. *Compare* Electronic Communications Privacy Act Amendments Act of 2011 § 3, *with* Electronic Communications Privacy Act, 18 U.S.C. § 2703 (a)–(b).

II. OVERVIEW OF CLOUD COMPUTING AND SMART GRID TECHNOLOGIES

A. *Cloud Computing*

Cloud computing is a technology that allows for an economically more efficient use of Information Technology (IT) resources.[11] The "cloud" is a data hosting method and consists of networks, remote data storage, and remote web-based applications.[12] Businesses and consumers use "webmail services, store data online, or . . . use software" applications having functionality in the cloud.[13] The cloud is where the remote IT applications, infrastructure, and platforms reside, rather than at an in-house data center.[14] The cloud could be a private network within an organization, a public network provided by a third party vendor, or a hybrid of both.[15] In a public network, the applications are hosted by a third party provider and are delivered to the end user via the Internet.[16] End users may view their files, pictures, movies, and emails at their visual display unit, which has access to the cloud.[17] This, in effect, gives users anywhere access to their applications and files stored by the third party provider.[18] Once information is stored in a third party cloud, it may be retrievable years later, even if the end user deletes the information.[19] A few of the major third party cloud-computing providers include Google, Amazon, Microsoft, and AT&T.[20]

It is estimated that over sixty-nine percent of people in our country use cloud computing for a variety of services.[21] Although there is a growing trend utilizing cloud computing, the technology behind cloud computing is

---

11. *See* Thethi, *supra* note 1, at 2.

12. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359, 360–61 (2010).

13. *Id.*

14. Marc Jonathan Blitz, Stanley *in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 HASTINGS L.J. 357, 366–67 (2010); *see* G Lakshmanan, *Cloud Computing: Relevance to Enterprise*, INFOSYS, 2 (2009), *available at* http://www.infosys.com/cloud/resource-center/documents/relevance-enterprise.pdf.

15. Thethi, *supra* note 1, at 2.

16. Soghoian, *supra* note 12, at 363–64.

17. Blitz, *supra* note 14, at 367.

18. *See* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2215 (2009).

19. *See* David S. Barnhill, Note, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 644 (2010); *Email*, SURVEILLANCE SELF-DEFENSE, http://ssd.eff.org/tech/email (last visited Apr. 15, 2012).

20. Soghoian, *supra* note 12, at 361; Anderson, *supra* note 3.

21. Soghoian, *supra* note 12, at 361.

not new.[22] Increases in processor and network speeds, coupled with the ability to store data inexpensively, provided the technology for cloud computing by the late 1990s.[23] Following this, virtualization enabled businesses to separate their software and hardware and run their applications remotely.[24] Virtualization was the impetus required to make cloud computing economically attractive and advantageous.[25]

Traditionally, many businesses have used an in-house data center IT model.[26] This required businesses to have enough capacity to handle peak requirements and pay the associated fixed costs of peak capacity.[27] Other fixed costs included the "cost of servers and storage, [in addition to] employee salaries and overhead."[28] Cloud computing offers flexibility and scalability, which enables businesses to only pay for what they actually use, or their variable costs.[29] The result is significant savings to businesses with respect to the fixed costs associated with hardware, software, facilities, and staff required for an in-house data center.[30]

It is projected that cloud computing will grow to account for a total public and private network spend of $33.1 billion by 2013.[31] There are some revenue projections as high as "$160 billion over the next few years."[32] It is also estimated that cloud computing technology will be deployed for the majority of IT services by 2020.[33]

B. *Smart Grid Technology*

Another technological area that is beginning to experience significant growth is smart grid technology.[34] With smart grid technology, utility companies are able to read meters remotely, reducing the costs of the staff and

22. Jim Cooke, *The Shift to Cloud Computing: Forget the Technology, It's About Economics*, CISCO, 1 (2010), *available at* http://www.cisco.com/web/about/ac79/docs/pov/Shift_to_Cloud_Computing_POV_IBSG.pdf.

23. *Id.* at 1–2.

24. *Id.* at 2.

25. *See id.*

26. *Id.* at 1.

27. *See* Cooke, *supra* note 22, at 2.

28. *Id.*

29. *Id.*; Thethi, *supra* note 1, at 2.

30. Cooke, *supra* note 22, at 2–3.

31. *Id.* at 5.

32. Soghoian, *supra* note 12, at 361.

33. Cooke, *supra* note 22, at 7.

34. *See* Kristi E. Swartz, *Energy Caution over Smart-Grid Security Southern Co. Says New Meters' Full Potential Needs Further Testing. Breaches Could Expose Data, Cause Blackouts*, ATLANTA J.-CONST., June 4, 2011, at A8.

transportation required to read a meter on site.[35] Energy usage may be tracked and managed not only by the utilities, but also by consumers.[36] The technology involves a decentralized system, two-way information flow, and two-way energy flow.[37] Smart grid technology requires a collaborative effort between "the IT industry, the telecom industry, the [I]nternet industry, the cyber-security industry, the appliance manufacturing industry, the meter manufacturing industry, and many more industries."[38] President Obama announced $3.4 billion in smart grid investment grants in 2009.[39] The United States Department of Energy predicts that over fifty-two million more meters will be installed by 2012.[40]

Experts in this area claim that the technology will result in a more efficient, secure, and reliable system.[41] It is predicted that with smart grid technology, electrical vehicles will "reduce our [country's] dependence on foreign oil by fifty-two percent."[42] Additionally, with smart grid, it is estimated that overall consumption will be reduced by up to four percent.[43] A few million metric tons of carbon dioxide is projected to be saved by 2030 with the use of smart grid, making it a green technology.[44] Furthermore, smart grid technology decreases the possibility of outages with its self healing characteristic, which would contribute to a significant cost savings because it is estimated that blackouts can account for $135 billion to commercial customers.[45] Finally, it is estimated that 280,000 jobs would be created with the implementation of smart grid technology.[46]

III. CURRENT LEGAL AND STATUTORY STANDARDS REGARDING PRIVACY

Privacy concerns affect both the cloud computing and smart grid technology industries.[47] Consumers and businesses may hesitate to subscribe to

35. *Id.*
36. *Id.*
37. *Energy Bar Association Panel Discussing the Smart Grid*, *supra* note 1, at 84.
38. *Id.* at 93.
39. Press Release, The White House, President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid (Oct. 27, 2009) (on file with The White House); Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 161 (2011).
40. Balough, *supra* note 39, at 162.
41. *Energy Bar Association Panel Discussing the Smart Grid*, *supra* note 1, at 85.
42. *Id.* at 88.
43. *Id.*
44. *Id.* at 88, 89.
45. *Id.* at 89.
46. *Energy Bar Association Panel Discussing the Smart Grid*, *supra* note 1, at 89.
47. Balough, *supra* note 39, at 162–63; Cooke, *supra* note 22, at 4.

services which expose them to the risk of unauthorized access to their private information.[48] Given the tremendous impact that the telecommunications and energy industries have on the economy, it would be ideal to address the privacy issues now, rather than later.[49]

A. *Privacy Issues and the Fourth Amendment*

End users of both cloud based and smart grid technologies are susceptible to privacy invasion.[50] The nature of cloud computing lends itself to the risk of insecure transmission of data.[51] Even with some forms of encryption, hackers are still able to access private information.[52] Risks to the end users are especially significant "when they [are] connect[ed] to . . . public wireless networks."[53]

Cloud computing services are not only exposed to cyber security issues involving potential hackers, but also are exposed to government access to private files and documents without a warrant in certain circumstances.[54] The Fourth Amendment states that:

> 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.[55]

Digital search and seizure using third party providers is much easier than retrieving documents from a personal computer.[56] In a digital environment, "law enforcement agents can obtain wiretaps, emails, text messages or real time phone location information."[57] It has previously been alleged that information from a third party cloud computing provider has been directly transmitted to government servers without a warrant.[58] In some cases, the government has been accused of having access to the entire network of a

48. *See* Balough, *supra* note 39, at 162–63; Cooke, *supra* note 22, at 4.
49. *See* Balough, *supra* note 39, at 161–65.
50. *Id.* at 165; Soghoian, *supra* note 12, at 361.
51. *See* Soghoian, *supra* note 12, at 361.
52. *See id.*
53. *Id.* at 372.
54. *Id.* at 361–62.
55. U.S. CONST. amend. IV.
56. Soghoian, *supra* note 12, at 386–87.
57. *Id.* at 385.
58. *Id.* at 385–86.

provider, which would enable the government to monitor an individual without involving the provider at all.[59]

Similarly, there are also privacy concerns with smart grid technology.[60] It is not absolutely clear just how much information the new and future smart meters will be able to accumulate.[61] The information obtained by the utility would include all of the energy consumed within a home and might also include additional information, such as the energy charged to an electric vehicle.[62] The electric vehicle would likely be registered to a user, or a unique identifier, so the data would follow the vehicle, even if it were charged somewhere else.[63] The information is gathered real-time for smart devices.[64] There are privacy implications when personal information—such as energy consumption within the home, and travel habits outside of the home—may potentially be tracked real-time.[65]

With smart grid technology, utilities currently use the Internet or other public networks to transfer the data.[66] The experts in the industry recognize that the smart grid system will be vulnerable to cyber attacks, and to authorized access to private information.[67] Additionally, "[u]tilities themselves [may also] pose a threat to . . . data" security through their internal monitoring and maintenance of the smart grid.[68] Other concerns with smart meters include the possibility of information remaining from previous homeowners, if not erased from the smart meter, and unauthorized landlord access in a rental situation.[69]

In the smart grid environment, law enforcement officials have previously used energy consumption data as an information tool.[70] The officials were able to use excessive energy consumption data to obtain warrants to access homes where they suspected marijuana might be grown because of the high energy usage.[71] Currently, it is not clear who owns the smart grid data—the end user or the utility.[72] Third party cloud computing providers and

59. *Id.* at 386.
60. Balough, *supra* note 39, at 162–63.
61. *Id.* at 165.
62. *Id.* at 166–67.
63. *Id.* at 167.
64. *Id.* at 166.
65. *See* Balough, *supra* note 39, at 165–67.
66. *Id.* at 168.
67. *See id.* at 169; *Energy Bar Association Panel Discussing the Smart Grid*, *supra* note 1, at 87.
68. Balough, *supra* note 39, at 169.
69. *Id.* at 171.
70. *Id.*
71. *Id.*
72. *Id.* at 173.

utilities similarly face the challenge of unauthorized access of private information and Fourth Amendment privacy issues.[73]

B. *ECPA Statutory Requirement*

Digital Due Process is a coalition of major carriers including: AT&T, AOL, Amazon, Microsoft, and others calling for a reform of the ECPA.[74] The ECPA is made up of "the Wiretap Act, the Stored Communications Act (SCA), and the use of pen register information."[75] Whether the government is required to obtain a search warrant, or only a court order, is determined by how the communication is interpreted.[76] If the communication is interpreted to fall under the Wiretap Act, then a search warrant is required.[77] On the other hand, if a communication falls within the SCA, only a court order may be required for government access.[78]

The main issue that the Digital Due Process coalition aims to address is the lack of a warrant requirement for a third party provider to disclose private communications and information to the government.[79] The coalition bases its argument on the need for Fourth Amendment protection in the cloud computing environment.[80] Quoting Justice Brandeis, the coalition emphasizes that privacy is "the most comprehensive of rights, and the right most valued by a free people."[81]

The ECPA does not clearly and effectively define how interception of modern day communications, such as email, should be treated.[82] By definition, a cloud computing provider is both an electronic communications service and a remote computing service.[83] An electronic communication service

73. Balough, *supra* note 39, at 165; Soghoian, *supra* note 12, at 361.

74. *About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Apr. 15, 2012); *Who We Are*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=DF652CE0-2552-11DFB455000C296BA163 (last visited Apr. 15, 2012).

75. Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 167 (2011).

76. *See id.*

77. *Id.*

78. *Id.*

79. *See Our Principles*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Apr. 15, 2012).

80. *About the Issue*, *supra* note 74.

81. *Id.*

82. Bagley, *supra* note 75, at 167–70.

83. *See id.* at 169.

provides users with the ability to send and receive electronic information.[84] A remote computing service, on the other hand, includes third party remote storage and applications.[85] Under the *United States Code* sections 2703(a) and 2703(b)(1)(B), after 180 days of an electronic communication, the government can compel a third party provider to release content information of that communication without a warrant and without the higher burden of probable cause.[86]

> [Section] 2703. Required disclosure of customer communications or records
>
> (a) Contents of Wire or Electronic Communications in Electronic Storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. *A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.*
>
> (b) Contents of Wire or Electronic Communications in a Remote Computing Service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

84. *See id.* at 167–68.

85. *See id.* at 168–69.

86. Electronic Communications Privacy Act, 18 U.S.C. § 2703(a)–(b)(1) (2006 & Supp. III 2009); *see* Bagley, *supra* note 75, at 168.

> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
>
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
>
> *(ii) obtains a court order for such disclosure under subsection (d) of this section;*
>
> *except that delayed notice may be given pursuant to section 2705 of this title.*[87]

The advances in technology have made the ECPA outdated and insufficient in addressing privacy concerns.[88] The standards have not been consistently applied by courts and there is no adequate protection of personal information.[89] The main changes in technology that are not adequately addressed by the ECPA are email, cell phone location data, cloud computing and social networking, and smart grid data.[90]

The ability of the government to obtain electronic communications from a service provider without a warrant requirement[91] demonstrates the problem that the coalition of Digital Due Process aims to correct.[92] There were seventeen class action cases in 2006[93] where the major telecommunications companies had allegedly partnered with the National Security Agency (NSA) to monitor phone calls and voluntarily provide information to the government.[94] The government had access to the information without obtaining a warrant.[95] The telecommunications companies were given legal protection when President Bush signed legislation granting immunity to the telecommunication

87. Electronic Communications Privacy Act, 18 U.S.C. § 2703(a)–(b)(1) (emphasis added).

88. *About the Issue*, *supra* note 74.

89. *Id.*

90. *Id.*

91. *See* Bagley, *supra* note 75, at 174.

92. *See Background*, DIGITAL DUE PROCESS, http://www.digitalddueprocess.org/index.cfm?objectid=C00D74C0-3C03-11DF-84C7000C296BA163 (last visited Apr. 15, 2012).

93. *In re* Nat'l Sec. Agency Telecomms. Records Litig., 444 F. Supp. 2d 1332, 1333 (J.P.M.L. 2006).

94. *See* Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 900 (N.D. Ill. 2006); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978, 988 (N.D. Cal. 2006); *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 444 F. Supp. at 1334.

95. *See Terkel*, 441 F. Supp. 2d at 900, 911; *Hepting*, 439 F. Supp. 2d at 978.

providers when assisting government in the fight on terrorism.[96] The NSA may have continued to intercept email and phone communications into 2009.[97]

Turning to the energy industry, the ECPA may provide some protections if a smart meter is considered to fall within the definitions under the Wiretap Act, where law officials would have to obtain a warrant for access to the information.[98] Under the Stored Communications Act, however, the level of privacy protection will depend on how the smart grid is defined.[99] If the smart grid is categorized as a remote computing service, then after 180 days of the data storage, the government could compel the utility to release the content of the information without a warrant.[100]

Given the technology movement toward remote storage of data, it is predictable that smart grid technology will ultimately be treated similar to cloud computing, i.e., as an electronic communication service and a remote computing service.[101] The technologies in the industries are converging in that there is an integration of IT and Operational Technology (OT).[102] "There is a strong push to . . . use . . . broadband, instead of utility-owned wires, for the transfer of smart meter data back to the utilities."[103] However, the technology currently available allows for the direct communication of the smart meter to the utility.[104] One supplier of smart meters explains:

> Gathering real-time data from intelligent endpoints provides the brainpower that drives the smart grid. [This supplier] outfits a variety of intelligent endpoints with its Communications Module to gather and relay this information. The . . . Communications

96. Bagley, *supra* note 75, at 157 n.16; James Risen, *Bush Signs Law to Widen Reach for Wiretapping: Restrictions Are Eased,* N.Y. TIMES, Aug. 6, 2007, at A1.

97. Bagley, *supra* note 75, at 159.

98. *See* Balough, *supra* note 39, at 177.

99. *Id.* at 179.

100. Electronic Communications Privacy Act, 18 U.S.C. § 2703(a)–(b)(1) (2006 & Supp. III 2009).

101. *See* Jesse Berst, *Breakthrough Best Practices for Blending IT and OT—Lessons from Duke and Accenture*, SMART GRID NEWS.COM (July 7, 2011), http://www.smartgridnews.com/artman/publish/Business_Lessons_Learned/Breakthrough-best-practices-for-blending-IT-and-OT----lessons-from-Duke-and-Accenture-3797.html.

102. *Id.*

103. Balough, *supra* note 39, at 168.

104. *See Intelligent Endpoints with Brains*, SILVER SPRING NETWORKS, http://www.silverspringnet.com/products/intelligent-endpoints.html (last visited Apr. 15, 2012).

> Modules support two connections—one into the utility's smart grid network and one into the consumer's home area network.[105]

In other words, the utility is able to gather the real-time data because the communicating devices, or intelligent endpoints, reside at the end user's home and at the utility.[106] This is analogous to a cloud computing provider gathering data communicated between a computer residing at a residence and the cloud. Therefore, it is predictable that the same privacy issues that are currently faced by the cloud computing providers will be faced by the utilities in the near future with the universal implementation of the smart grid.[107]

C. Katz v. United States *and the Reasonable Expectation of Privacy Test*

The modern standard for privacy with regard to electronic surveillance is based on *Katz*.[108] In *Katz*, the FBI attached an electronic listening and recording device to the outside of a phone booth and monitored the petitioner's conversations during phone calls he made while in the phone booth.[109] The Supreme Court of the United States was asked to address whether a public telephone booth is a protected area of an individual's right to privacy.[110] The Court reasoned that "the Fourth Amendment protects people, not places."[111] The Court stated:

> One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[112]

---

105. *Id.*

106. *Id.*; *see* News Release, AT&T, AT&T to Offer Wireless Smart Grid Technology to Utility Companies (Mar. 17, 2009), *available at* http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=26613&mapcode=enterprise/mk-att-sustainability.

107. *See* Balough, *supra* note 39, at 161–62, 171–72.

108. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010).

109. Katz v. United States, 389 U.S. 347, 348 (1967).

110. *Id.* at 349.

111. *Id.* at 351.

112. *Id.* at 352.

The standard explained in Justice Harlan's concurring opinion in *Katz* is followed today and is the reasonable expectation of privacy test.[113] The reasonable expectation of privacy standard has two prongs.[114] Under the first prong, an individual must subjectively have an expectation of privacy.[115] Under the second objective prong, society would have to recognize it as a reasonable expectation of privacy.[116]

There has been criticism of the subjective nature of the *Katz* test and some inconsistent results in applying the reasonable expectation of privacy standard.[117] For example, in *Oliver v. United States*,[118] the Supreme Court of the United States held that a person does not have a reasonable expectation of privacy for activities conducted in fields that could have been seen by lawful aerial surveillance.[119] In *Oliver*, two agents approached a farmhouse, followed a footpath around a locked gate, and entered into a field where marijuana was grown.[120] The Court explained that an expectation of privacy in open fields is not one that society would recognize as reasonable.[121] The Court held that no expectation of privacy attaches to open fields.[122]

However, in *Bond v. United States*,[123] the Court distinguished between visual and tactile observation of property.[124] In *Bond*, a bus passenger's luggage was placed in the overhead storage area.[125] A border patrol agent squeezed the luggage as he walked through the bus.[126] The Court applied the two pronged reasonable expectation of privacy test.[127] Under the first prong, the passenger was found to expect privacy because he placed his belongings in an opaque bag and positioned the bag directly above him.[128] Under the second prong, the Court explained that a bus passenger may expect some handling of the bag, but not handling in an exploratory manner.[129] The Court

113. Solove, *supra* note 108, at 1511 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).
114. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
115. *Id.*
116. *Id.*
117. Kyllo v. United States, 533 U.S. 27, 34 (2001).
118. 466 U.S. 170 (1984).
119. *Id.* at 178–79.
120. *Id.* at 173.
121. *Id.* at 179.
122. *Id.* at 180.
123. 529 U.S. 334 (2000).
124. *Id.* at 337.
125. *Id.* at 335.
126. *Id.*
127. *Id.* at 338.
128. *Bond*, 529 U.S. at 338.
129. *Id.* at 338–39.

held that the physical manipulation of the bus passenger's luggage violated the Fourth Amendment, even though the bag was exposed to public handling in an overhead compartment.[130]

Additionally, in *Kyllo v. United States*,[131] law enforcement used a thermal imaging device to detect the heat generated from lamps used for indoor marijuana growth.[132] The Court held that this was an intrusion into the protected area and would constitute a search.[133] The Court also emphasized that this type of technology is not in general public use.[134] The Court stated that the "[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment."[135] Justice Stevens, dissenting, argued that heat waves that are generated "enter the public . . . if and when they leave a building."[136] According to the dissent, "[a] subjective expectation that [heat waves] would remain private is not only implausible, but also surely not 'one that society is prepared to recognize as reasonable.'"[137]

Most recently, in *United States v. Jones*,[138] the Supreme Court of the United States reverted to trespass analysis in deciding that the physical attachment of a GPS tracking device on the defendant's vehicle constituted a trespass of a constitutionally protected "effect."[139] The Supreme Court of the United States did not apply the *Katz* test, but explained that "unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test."[140] Therefore, the *Katz* reasonable expectation of privacy test continues to apply.[141]

130. *Id.*
131. 533 U.S. 27 (2001).
132. *Id.* at 29.
133. *Id.* at 34.
134. *Id.*
135. *Id.* at 35 n.2.
136. *Kyllo*, 533 U.S. at 43–44 (Stevens, J., dissenting).
137. *Id.* at 44 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).
138. No. 10-1259, slip op. (U.S. Jan. 23, 2012).
139. *Id.* at 4, 10 & n.8.
140. *Id.* at 11 (emphasis in original).
141. *Id.*

D. *Supreme Court of the United States Evades Fourth Amendment Issue in* City of Ontario v. Quon

There is not a significant amount of case law applying Fourth Amendment protection in electronic communications.[142] Some believe that the current case law "leaves more questions than answers" regarding whether the Fourth Amendment applies in government access to electronic communications.[143] The Supreme Court of the United States had an opportunity in *Quon* to address issue of Fourth Amendment protection with respect to text messaging.[144]

In *Quon*, a city employee claimed that his Fourth Amendment privacy rights were violated when the city "read text messages sent and received on [his] pager."[145] The Supreme Court of the United States avoided taking a stand on the Fourth Amendment issues.[146] "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[147] Because the pager was owned and issued to the employee from the employer, the Court explained that "prudence counsels caution" in defining privacy expectations of employees using employer provided communication devices.[148] Although the Court acknowledged that cell phone and text message communications are highly personal, the Court also explained that these devices could be purchased by individuals themselves.[149]

The Court reasoned that there are exceptions to the general rule of warrantless searches, and that "'special needs' of the workplace justify one such exception."[150] The issue of whether there was a reasonable expectation of privacy was not necessary to resolve[151] because the Court held that the city's review of its employee's text messages was reasonable under the exception regarding "'special needs' of the workplace."[152] Therefore, the reasonable expectation of privacy regarding electronic communications has not been clearly addressed by the Supreme Court of the United States.[153]

---

142. *See* Blitz, *supra* note 14, at 372.
143. Bagley, *supra* note 75, at 171.
144. City of Ontario v. Quon, 130 S. Ct. 2619, 2624 (2010).
145. *Id.* at 2624.
146. Blitz, *supra* note 14, at 373.
147. *Quon*, 130 S. Ct. at 2629.
148. *Id.*
149. *Id.* at 2630.
150. *Id.* (quoting O'Connor v. Ortega, 480 U.S. 709, 725 (1987)).
151. *See id.*
152. *Quon*, 130 S. Ct. at 2630.
153. *See id.*

E. *The Third Party Doctrine*

The third party doctrine is thought by some to be "disguised as an application of *Katz's* 'reasonable expectation of privacy'" standard.[154] The logic in support of the third party doctrine is that if an individual discloses information to a third party, then it is not reasonable for the individual to have an expectation of privacy.[155] The third party doctrine is pertinent to third party cloud computing providers, and will be pertinent to smart grid utilities, because data is turned over to and stored remotely by the third party providers.[156]

In *Smith v. Maryland*,[157] telephone numbers dialed from the petitioner's home were recorded using a pen register installed by the telephone company at the request of the police.[158] The police did not obtain a warrant or court order for access to the information.[159] The Supreme Court of the United States distinguished a pen register from the listening device in *Katz*, because the register only disclosed the telephone numbers that the petitioner dialed not the conversations.[160] The Court reasoned that by disclosing the telephone numbers to the phone company, the petitioner could not have a reasonable expectation of privacy because the phone company uses the information to complete the calls and bill the end user.[161]

Likewise, in *United States v. Miller*,[162] a bank provided the petitioner's checks, deposit slips, financial statements and monthly statements to agents.[163] The Supreme Court of the United States differentiated between an individual's private papers and the bank's business records.[164] The Court further explained that the documents contained only information willingly communicated to the bank.[165] Justice Powell stated that "[t]he depositor

154. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009).

155. *Id.* at 563; *see* United States v. Miller, 425 U.S. 435, 443 (1976), *superseded by statute*, Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3697, *as recognized in* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984).

156. Couillard, *supra* note 18, at 2215.

157. 442 U.S. 735 (1979).

158. *Id.* at 737.

159. *Id.*

160. *Id.* at 741.

161. *Id.* at 742.

162. 425 U.S. 435 (1976), *superseded by statute*, Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3697, *as recognized in* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984).

163. *Id.* at 438.

164. *Id.* at 440.

165. *Id.* at 442.

takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to [another]."[166]

Critics of the third party doctrine claim that it is incorrectly applied to the *Katz* test.[167] It has been argued that it is reasonable to "expect privacy [of] bank records, phone records, and other third-party records."[168] Another view is that the third party doctrine gives the government too much power.[169] With the advances in technology and public access to the Internet, the third party doctrine is thought to be insufficient in addressing the modern information era.[170] An additional criticism is that the doctrine was articulated prior to data storage in the cloud and should not apply to a third party provider and its end users.[171]

On the other hand, benefits of the third party doctrine may often be overlooked.[172] Some contend that the rule ensures "technological neutrality in Fourth Amendment rules."[173] For example, the third party doctrine prevents criminals from conducting their crimes privately and hiding the public aspects of those crimes.[174] Without the third party doctrine, criminals would be enabled to conceal their crimes.[175] Another argument in defense of the third party doctrine is that when users divulge information to a third party, they are impliedly consenting under the Fourth Amendment.[176]

F. *Reasonable Expectation of Privacy in the Cloud*

The question is, "when do people have a reasonable expectation of privacy in data stored in the cloud?"[177] Likewise, when will people have a reasonable expectation of data generated from a smart meter? Some view the Internet as a public space where there can be no reasonable privacy expectation.[178] However, several factors support an individual having a reasonable expectation of privacy in using third party providers.[179] First, a user account

166. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).
167. Kerr, *supra* note 154, at 570.
168. *Id.* at 571.
169. *Id.* at 572.
170. *See id.* at 573.
171. Bagley, *supra* note 75, at 174.
172. Kerr, *supra* note 154, at 573.
173. *Id.*
174. *Id.*
175. *Id.*
176. Bagley, *supra* note 75, at 175.
177. Barnhill, *supra* note 19, at 621.
178. Couillard, *supra* note 18, at 2221.
179. *See* Bagley, *supra* note 75, at 176–77.

is typically protected by a password and personal login.[180] Password protection, in itself, would lead one to have an expectation of privacy.[181] In addition, an individual's private account is not accessible to public view.[182] Furthermore, the nature of photographs, calendars, and other private files is highly personal.[183] Moreover, it is reasonable to have an expectation of privacy when conducting a search for information on the Internet in the privacy of one's home, or in the privacy of using one's personal devices.[184]

Individuals' privacy expectations are no longer confined to the protected area of the home, but also include their password-protected activities and accounts.[185] However, "web searches, emails, documents, photos, location data, and even evidence of acquaintanceship can be extracted from a user account."[186] Data from calendars, voicemails and instant message logs are also retrievable.[187] It has been suggested that this type of information could even possibly be used for criminal profiling.[188]

The third party doctrine has not been adapted for the post-*Katz* cloud computing environment, nor has it been adapted for the smart grid era.[189] The third party doctrine must take into account modern society's expectations that private password protected information, whether stored remotely or on a desktop, or generated from a smart meter is not accessible to the general public.[190] Some contend that "[l]ooking at expectations is the wrong inquiry" all together.[191]

180. *Id.* at 176.
181. *Id.*
182. *Id.*
183. Couillard, *supra* note 18, at 2219–20.
184. Bagley, *supra* note 75, at 170–71.
185. *Id.* at 170.
186. *Id.* at 161.
187. *Id.* at 162.
188. *Id.* at 164.
189. Couillard, *supra* note 18, at 2219.
190. *Id.* at 2231–32.
191. Solove, *supra* note 108, at 1524.

IV. PROPOSED STATUTORY REQUIREMENTS REGARDING PRIVACY AND POTENTIAL EXCEPTIONS

A. *The Proposed Electronic Communications Privacy Act Amendments Act of 2011*

Proposed legislation, introduced in May 2011, attempts to address some of the privacy concerns with respect to electronic communications.[192] The Electronic Communications Privacy Act Amendments Act of 2011 aims to "improve the provisions relating to the privacy of electronic communications."[193] This paper focuses on sections two and three of the bill:

> Sec. 2. Prohibition on Disclosure of Content.
>
> Section 2702(a)(3) of title 18, United States Code, is amended to read as follows:
>
> (3) A provider of electronic communication service, remote computing service, or geolocation information service to the public shall not knowingly divulge to any governmental entity the contents of any communication described in section 2703(a), or any record or other information pertaining to a subscriber or customer of such provider or service.
>
> Sec. 3. Elimination of 180-Day Rule and Search Warrant Requirement; Required Disclosure of Customer Records.
>
> (a) In General.—Section 2703 of title 18, United States Code, is amended—
>
> (1) by striking subsections (a), (b), and (c) and inserting the following:
>
> (a) Contents of Wire or Electronic Communications in Electronic Storage.—
>
> (1) In general.—A governmental entity may require the disclosure by a provider of electronic communication service, remote computing service, or geolocation information service of the contents of a wire or electronic communication that is in electronic

192. *See generally* Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011).

193. *Id.*

storage with or otherwise held or maintained by the provider if the governmental entity obtains a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure.

(2) Notice.—Except as provided in section 2705, not later than [three] days after a governmental entity receives the contents of a wire or electronic communication of a subscriber or customer from a provider of electronic communication service, remote computing service, or geolocation information service under paragraph (1), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

(A) a copy of the warrant; and

(B) a notice that includes the information referred to in section 2705(a)(5)(B)(i).

(b) Records Concerning Electronic Communication Service, Remote Computing Service, or Geolocation Information Service.—

(1) In general.—Subject to paragraph (2) and subsection (g), a governmental entity may require a provider of electronic communication service, remote computing service, or geolocation information service to disclose a record or other information pertaining to a subscriber or customer of the provider or service (not including the contents of communications), only if the governmental entity—

(A) obtains a warrant issued and executed in accordance with the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure;

(B) obtains a court order directing the disclosure under subsection (c);

(C) has the consent of the subscriber or customer to the disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the

> name, address, and place of business of a subscriber or customer of the provider or service that is engaged in telemarketing (as defined in section 2325).[194]

The proposed legislation addresses the search warrant requirement for contents of electronic communications stored by cloud computing providers.[195] However, it does not attempt to include smart grid technology.[196] It is not clear how the smart meter would be defined.[197] The proposed legislation should include consideration for smart meter technology because it seems that the energy industry will be faced with the same Fourth Amendment privacy issues as the telecommunications providers.[198] Otherwise, the courts will be left struggling with whether a smart meter may be categorized as an electronic communication service, remote computing service, or geolocation information service.[199] It would be a better use of resources to address these industries and technologies together, based on the synergies of the industries and the interests of the taxpayers for efficient use of government and judicial resources.[200]

B. *Exceptions for the Proposed Legislation to Consider*

As mentioned previously, the third party doctrine is thought to be insufficient in addressing the modern information era.[201] If the proposed legislation passes, it will clearly establish a warrant requirement for government access to the content of stored third party cloud information.[202] However, in addition to the third party doctrine, there are two other exceptions that should be considered in addressing the modern information era—the independent source doctrine and the inevitable discovery rule.[203] If the above proposed legislation is adopted, and a warrant is required for access to the information stored in the cloud or with a third party, then the independent source doctrine and the inevitable discovery rule may undermine its purpose.

---

194. *Id.* §§ 2–3.
195. *See id.*
196. *See id.*
197. Balough, *supra* note 39, at 172.
198. *Id.*
199. *See id.*
200. *See* Berst, *supra* note 101.
201. Kerr, *supra* note 154, at 573.
202. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. §§ 2–3 (2011).
203. Segura v. United States, 468 U.S. 796, 805 (1984); Nix v. Williams, 467 U.S. 431, 444 (1984).

1. The Independent Source Doctrine

Under the independent source doctrine, evidence that is first discovered unlawfully, but later is obtained in a lawful manner that is independent of the first discovery, is admissible.[204] In *Segura v. United States*,[205] the Supreme Court of the United States addressed the issue of whether items discovered by agents under a valid search warrant, following an unlawful entry, should be suppressed from evidence.[206] In *Segura*, agents entered into and remained in an apartment for nineteen hours awaiting a search warrant while the lawful occupants were taken into police custody.[207] After the warrant issued, the agents discovered drugs, ammunition, cash, and records.[208] The Court held that the evidence discovered pursuant to the warrant was admissible, and only the evidence that was discovered prior to the warrant was suppressed.[209] The Court reasoned that none of the information on which the warrant was secured was derived from the initial entry, and the information was known to the agents prior to the entry.[210] The Court stated that "the exclusionary rule has no application [where] the Government learned of the evidence 'from an independent source.'"[211]

In *Murray v. United States*,[212] federal agents entered a warehouse, without a warrant, to apprehend those who were seen from surveillance within the warehouse.[213] The agents forced entry and did not find the individuals, but they did view burlap-wrapped bales of marijuana in plain sight.[214] The agents left the warehouse under surveillance and then obtained a search warrant.[215] The search warrant did not rely on the observations made in the first unlawful entry of the warehouse and was considered to be untainted.[216] The Court explained that the independent source doctrine may apply to evidence acquired through Fourth, Fifth, and Sixth Amendment violations.[217] The doctrine's aim is to protect society's interest of allowing juries to receive

204. *Segura*, 468 U.S. at 805.
205. 468 U.S. 796 (1984).
206. *Id.* at 804.
207. *Id.* at 800–01.
208. *Id.* at 801.
209. *Id.* at 813–14, 816.
210. *Segura*, 468 U.S. at 814.
211. *Id.* at 805 (quoting Wong Sun v. United States, 371 U.S. 471, 487 (1963)) (internal quotation marks omitted).
212. 487 U.S. 533 (1988).
213. *Id.* at 535.
214. *Id.*
215. *Id.* at 535–36.
216. *See id.* at 535–37.
217. *Murray*, 487 U.S. at 537.

evidence of a crime by putting police in the same position they would have been in if no violation occurred.[218]

> "[T]he interest of society in deterring unlawful police conduct and the public interest in having juries receive all probative evidence of a crime are properly balanced by putting the police in the same, not a worse, position that they would have been in if no police error or misconduct had occurred. . . . When the challenged evidence has an independent source, exclusion of such evidence would put the police in a worse position than they would have been in absent any error or violation."[219]

In *Murray*, Justice Scalia explained that "[t]o determine whether [a] warrant was independent of the illegal entry, [the question is] whether it would have been sought even if what actually happened had not occurred."[220]

In *Hudson v. Michigan*,[221] the Supreme Court of the United States also applied the independent source doctrine.[222] In *Hudson*, there was a valid warrant, but it was executed in violation of the knock and announce rule.[223] Justice Scalia compared the search to the warrantless search in *Segura*.[224] He stated that "[i]f the probable cause backing a warrant that was issued *later in time* [in *Segura*] could be an 'independent source' for a search that proceeded after the officers illegally entered and waited, a search warrant obtained before going in must have at least this much effect."[225]

2. The Inevitable Discovery Rule

The inevitable discovery rule is inferred from the independent source doctrine.[226] The main difference is that with the inevitable discovery doctrine, derivative evidence is permissible if the police would have *hypothetically* discovered the evidence lawfully.[227] The prosecutor must show that by a preponderance of the evidence, the challenged evidence would inevitably

218. *Id.* (quoting Nix v. Williams, 467 U.S. 431, 443 (1984)).
219. *Id.* (alteration in original) (emphasis omitted) (quoting *Nix*, 467 U.S. at 443).
220. *Id.* at 542 n.3.
221. 547 U.S. 586 (2006).
222. *See id.* at 600–01.
223. *Id.* at 588, 590.
224. *Id.* at 600–01.
225. *Id.* (emphasis omitted).
226. Murray v. United States, 487 U.S. 533, 539 (1988).
227. Nix v. Williams, 467 U.S. 431, 443–44 (1984).

"have been discovered by lawful means."[228] Probable cause must have been established for the application of inevitable discovery.[229]

In *Nix v. Williams*,[230] the location of a body was disclosed to law enforcement in violation of the defendant's right to counsel.[231] Although *Nix* is a Sixth Amendment case, the reasoning may logically apply to Fourth Amendment cases as well.[232] In the inevitable discovery situation, there is a causal connection between the illegality and the acquisition of the evidence.[233]

In *Nix*, a nearby search team was within a few miles of discovering the body, but was called off after the defendant brought the police to where the body was buried.[234] The Supreme Court of the United States reasoned that it was inevitable that the body would have been found by the search team.[235] The Court justified adopting the inevitable discovery rule based on the rationale of the independent source exception.[236] The underlying reasoning of both doctrines is to allow evidence that would have been available absent any unlawful police activity.[237] *Nix* was decided in 1984, at a time the Court believed that "[a] police officer who is faced with the opportunity to obtain evidence illegally will rarely, if ever, be in a position to calculate whether the evidence sought would inevitably be discovered."[238]

In one lower court decision, *United States v. Rodriguez*,[239] one of the defendants, King, made a statement under duress, which led to derivative evidence.[240] The court relied on the inevitable discovery exception, and reasoned that "[u]pon consideration of all the circumstances surrounding this search, I conclude that a team of well trained and experienced law enforce-

228. *Id.* at 444.
229. *See id.* at 443–44.
230. 467 U.S. 431 (1984).
231. *Id.* at 435–37.
232. 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE 388 (5th ed. 2010) ("Although the violation in *Nix* involved the Sixth Amendment right to counsel, the . . . analysis applies in the same manner in Fourth Amendment cases."). Additionally, the inevitable discovery doctrine is inferred from the independent source doctrine, which does apply to Fourth, Fifth, and Sixth Amendment cases. Murray v. United States, 487 U.S. 533, 537 (1988).
233. *Nix*, 467 U.S. at 444.
234. *Id.* at 436.
235. *Id.* at 449–50.
236. *Id.* at 444.
237. *Id.* at 443–45.
238. *Nix*, 467 U.S. at 431, 445.
239. 606 F. Supp. 1363 (D. Mass. 1985).
240. *Id.* at 1374.

ment officers would have discovered the . . . evidence without King's assistance."[241]

C. *Applying the Exceptions to the Proposed Legislation*

In effect, the independent source and inevitable discovery rules are exceptions that may potentially undermine the proposed search warrant requirement for electronic communications in certain instances.[242] There are main features of electronic communications that differentiate electronic communications from traditional paper sources and other types of evidence: Processability, recoverability, and remote storage.[243] "Electronic [e]vidence [i]s [a]lways [p]rocessable."[244] Traditional paper documents must be manually searched through, whereas electronic communications may be electronically searched for within seconds.[245] In addition to traditional searching, modern technology also allows for data mining, where patterns within data are identified.[246] Furthermore, it is possible to recover, preserve, and reproduce deleted files in electronic communications.[247] These features coupled with cloud computing technology, where files are remotely stored, are characteristics unique to electronic communications.[248] The outdated inquiries and standards for the independent source doctrine and the inevitable discovery rule are less burdensome in electronic evidence because of the characteristics of electronic communications.

1. Application of the Independent Source Doctrine to the Proposed Warrant Requirement

The question in *Murray* of whether a warrant "would have been sought even if what actually happened had not occurred,"[249] opens the door in the electronic world to hack now, get a warrant later.[250] The Court in *Murray*

241. *Id.* at 1375.
242. *See, e.g.*, State v. Williamson, 701 So. 2d 1243, 1245 (Fla. 5th Dist. Ct. App. 1997).
243. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 364–65 (2000).
244. *Id.* at 364.
245. *Id.*
246. *Data Mining*, DATATRIAGE, http://www.datatriage.com/data_mining.php (last visited Apr. 15, 2012).
247. *Specialized Hard Drive Data Recovery Services*, DATATRIAGE, http://datatriage.com/hard_drive_recovery.php (last visited Apr. 15, 2012).
248. *See* Scheindlin & Rabkin, *supra* note 243, at 364.
249. Murray v. United States, 487 U.S. 533, 542 n.3 (1988).
250. *See id.* at 540 n.2.

explained that the lawfully obtained search warrant did not rely on the observations made in the first unlawful entry of the warehouse.[251] In an electronic communications environment, if there is an unlawful access to electronic information stored by a third party, followed by a lawfully obtained warrant, there is a potential argument that the lawfully obtained warrant "would have been sought even if what actually happened had not occurred."[252] The characteristics of electronic communications support the idea that the lawfully obtained warrant would not have relied on the observations made by the first unlawful access to the information.[253] The reasoning in support of this hypothetical argument is that the second lawfully obtained warrant would have been obtained based on the search criteria—which for this analysis assumes was sufficient to give rise to probable cause—used to access the electronic communication in the first unlawful access.

There are unique processes in place for investigators to conduct a search through Internet service providers.[254] For example, when dealing with Internet service providers, the agent determines what material the provider is to retrieve, but the agent usually does not conduct the search of the provider's computers.[255] The agent "serve[s] the warrant on the provider, . . . and the provider produces the material specified in the warrant."[256] In order to navigate through massive volumes of electronic documents,[257] the provider would use the information provided by the agent to conduct the search.[258] Next, the agent reviews the information retrieved, and makes copies of what the agent believes falls within the scope of the warrant.[259] It follows that if an agent started with sufficient information to give rise to probable cause, and that information led to search criteria to be used by a provider in order to retrieve the electronic communications, then the search criteria would always be an independent source of what is actually retrieved.

For example, in the personal computer environment, if an agent obtains an IP address from a victim's computer, after a cyber crime has been com-

251. *Id.* at 541–43.

252. *See id.* at 542–43 & 542 n.3.

253. *Id.* at 542–43.

254. *See* U.S. DEP'T OF JUST., COMPUTER CRIME & INTELLECTUAL PROP. SEC. CRIMINAL DIV., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 133–34 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

255. *Id.* at 134.

256. *Id.* (citing Electronic Communications Privacy Act, 18 U.S.C. § 2703(g) (2006 & Supp. III 2009)).

257. *See* Scheindlin & Rabkin, *supra* note 243, at 364.

258. U.S. DEP'T OF JUST., *supra* note 254, at 134.

259. *Id.*

mitted, and the agent, pursuant to a subpoena, compels the Internet service provider to provide the name and address associated with the IP address, and verifies the address, then with that information the agent typically has probable cause to search the suspect's home computer.[260] Electronic communications associated with the suspect would also likely be stored in the cloud.[261] By analogy, the agent in this example would have the same probable cause to search the cloud for the electronic communications. In other words, if the information gives rise to probable cause to search the suspect's home computer, it will also give rise to probable cause to search the suspect's material stored in the cloud. The sufficient information used to search and acquire the electronic communication in the cloud would be known to the agent prior to the search in the cloud.

The independent nature of an electronic communication search is consistent with the reasoning in *Segura*, where the Court stated that the information was known to the agents prior to the entry, and was, therefore, an independent source.[262] The characteristic of electronic communications being processable, based on entered search terms, supports the notion that the electronic communications "would have been sought even if what actually happened had not occurred."[263] Without a focused search at the outset containing specific information, there would be potentially millions of pages of retrievable text stored as electronic documents.[264] Assuming the agent has sufficient information to give rise to probable cause in formulating the search criteria, the search would not be based on information found in the material generated by the search.[265]

In defending against the criticism that the independent source doctrine fosters a "search first, warrant later mentality," Justice Scalia notes that:

---

260. *Id.* at 65.

> In a common computer search scenario, investigators learn of online criminal conduct. Using records obtained from a victim or from a service provider, investigators determine the Internet Protocol ("IP") address used to commit the crime. Using a subpoena . . . investigators then compel the Internet Service Provider ("ISP") that has control over that IP address to identify which of its customers was assigned that IP address at the relevant time, and to provide (if known) the user's name, street address, and other identifying information. In some cases, investigators confirm that the person named by the ISP actually resides at that street address by, for example, conducting a mail cover or checking utility bills.
>
> Affidavits that describe such an investigation are typically sufficient to establish probable cause . . . .

Id.

261. *See* Couillard, *supra* note 18, at 2215.

262. Segura v. United States, 468 U.S. 796, 814 (1984).

263. Murray v. United States, 487 U.S. 533, 542 n.3 (1988).

264. *See* Scheindlin & Rabkin, *supra* note 243, at 366–67.

265. *See* U.S. DEP'T OF JUST., *supra* note 254, at 134.

> An officer with probable cause . . . would be foolish to enter the premises first in an unlawful manner. By doing so, he would risk suppression of all evidence . . . [and would have] the much more onerous burden of convincing a trial court that no information gained from the illegal entry affected . . . the law enforcement officers' decision to seek a warrant . . . .[266]

Based on the processable nature of electronic communications, the burden of convincing a trial court that there was no information gained from the illegal access to electronic communications may be lessened, because in order to have retrieved the documents there must have been information obtained prior to and independent of the search to conduct the search.[267] If the information used to conduct the search was sufficient to give rise to probable cause, and the information was used to identify search criteria, then the information was known prior to and independent of the search. Therefore, the risk for the officer that Justice Scalia refers to, in effect, may not be as great as it would be in dealing with others forms of evidence.[268]

2. Application of the Inevitable Discovery Rule to the Proposed Warrant Requirement

At the time *Nix* was decided, electronic communication as we know it today did not exist. The reasoning in *Nix* that "[a] police officer who is faced with the opportunity to obtain evidence illegally will rarely, if ever, be in a position to calculate whether the evidence sought would inevitably be discovered"[269] does not apply in an electronic communication world where evidence can be backed up, restored, "mined" for patterns and irregularities, and remotely stored.[270] Stored data, on a third party computer, may be backed up by the third party for disaster recovery purposes, which allows for restoral of data to a previous date.[271] Additionally, even if an end user deletes an electronic file, it can still technically be recovered with computer forensic services.[272] Furthermore, with data mining technology available, patterns in data will reveal information that otherwise would not be obvious.[273]

---

266. *Murray*, 487 U.S. at 540 n.2, 540.
267. *Cf. id.* at 540, 542 n.3.
268. *See id.* at 539, 540.
269. Nix v. Williams, 467 U.S. 431, 445 (1984).
270. *See, e.g.*, Barnhill, *supra* note 19, at 644; *see Data Mining*, *supra* note 246.
271. *See* Barnhill, *supra* note 19, at 644.
272. *Specialized Hard Drive Data Recovery Services*, *supra* note 247.
273. *Data Mining*, *supra* note 246.

> Data mining is a special process used to search electronic stored information (ESI). The results of the data mining process will help direct future actions in the discovery process prior to litigation. Generally data mining refers to searching large volumes of data for patterns and irregularities in the data. The patterns and irregularities found, in turn, trigger yet more detailed searches within the data.[274]

In order to satisfy the inevitable discovery doctrine, the prosecutor only has the burden of a preponderance of the evidence showing that the electronic communication and its contents "would have been [found] by lawful means."[275] Again, assuming there is sufficient information to obtain a warrant, an agent has the technical ability to process, recover, or access a remote copy in the cloud.[276] In electronic communications, these characteristics increase the likelihood that the electronic communication and its contents would have been found with a lawfully obtained warrant.[277] This may suggest that an officer would be placed in a position to accurately calculate whether the evidence sought would inevitably be discovered, which undermines the court's reasoning in *Nix*.[278]

In applying *Rodriguez*, where the judge believed that a well trained team would have discovered the evidence regardless of King's statements,[279] there is a circular reasoning in electronic communications because of the processable, restorable, and remotely stored cloud characteristics.[280] In the case where there is sufficient probable cause for a search, a well trained team would almost always have been able to discover documents that are stored in the cloud.[281] The reasoning that applies in the inevitable discovery doctrine becomes circular when applied to electronic communications.[282]

For example, an inevitable discovery argument may arise when a lawfully seized device contains information that may also be stored in the cloud, such as email account information.[283] A potential argument is that the material relating to that account information is stored in the cloud and would be

274. *Id.*
275. Nix v. Williams, 467 U.S. 431, 444 (1984).
276. *See* Barnhill, *supra* note 19, at 644.
277. *See id.*
278. *Compare Nix*, 467 U.S. at 445, *with* Barnhill, *supra* note 19, at 644.
279. United States v. Rodriguez, 606 F. Supp. 1363, 1375 (D. Mass. 1985).
280. *Compare Nix*, 467 U.S. at 445, *with* Barnhill, *supra* note 19, at 644.
281. *Compare Rodriguez*, 606 F. Supp. at 1374–75 *with* Barnhill, *supra* note 19, at 644.
282. *Compare Nix*, 467 U.S. at 445, *with* Barnhill, *supra* note 19, at 644.
283. *See* Government's Response to Defendant's Notice to Suppress Evidence of Defendant Bickle's Emails at 15, United States v. Bickle, No. 2:10-CR-565-RLH-PAL, 2011 WL 3798225 (D. Nev. July 21, 2011).

inevitably discovered.[284] In one such case, emails were obtained from Microsoft by the government with a warrant.[285] The defendant claimed that the warrant lacked probable cause to believe that the email account would contain relevant evidence.[286] The government responded that even if the warrant lacked probable cause, the court should deny the motion to suppress based on inevitable discovery.[287] The government had lawfully seized the defendant's cellular telephone which had email information stored on it.[288] The government argued that "[t]o the extent that [the] email account information stored on the defendant's seized telephone overlaps with [the] email account information obtained through the search [through Microsoft] at issue here, the [c]ourt should not suppress that information."[289] The court did not need to address the inevitable discovery issue.[290] Nevertheless, the government's argument was that inevitable discovery should apply where the email account information was unlawfully obtained from the cloud provider, because the email account information was lawfully obtained through another device, and would have inevitably lead to the information in the cloud.[291]

The aforementioned processable, recoverable, and remotely stored characteristics support the idea that where probable cause exists, the electronic communication and its contents would have been inevitably found with a lawfully obtained warrant, regardless of a prior unlawful access.[292] The underlying aim of both the independent source doctrine and the inevitable discovery rule is to protect society by putting police in the same position they would have been in if no violation occurred.[293] The nature of electronic communications and applications in the cloud may put police in the same position as they would have been in if no search warrant violation had occurred because of the unique characteristics of electronic communications.[294]

284. *See id.*

285. United States v. Bickle, No. 2:10-cr-00565-RLH-PAL, 2011 WL 3798225, at *1 (D. Nev. June 21, 2011).

286. *Id.* at *1–2.

287. Government's Response to Defendant's Notice to Suppress Evidence of Defendant Bickle's Emails, *supra* note 283, at 15.

288. *Id.*

289. *Id.* at 16.

290. *See* Bickle, 2011 WL 3798225, at *5, *22–23.

291. Government's Response to Defendant's Notice to Suppress Evidence of Defendant Bickle's Emails, *supra* note 283, at 15.

292. *See id.* at 15–16 (citing Nix v. Williams, 467 U.S. 431, 444 (1984)).

293. *See* Murray v. United States, 487 U.S. 533, 541 (1988).

294. *See* Barnhill, *supra* note 19, at 644–45.

V. CONCLUSION

The Obama administration opposes changes to the existing ECPA, which would make it more difficult for the government to obtain access to the content of electronic communications.[295] "[T]he Obama administration testified that imposing constitutional safeguards on email stored in the cloud would be an unnecessary burden on the government. Probable-cause warrants would only get in the government's way."[296] Nevertheless, the economy would benefit if more users felt secure about cloud computing, and storing their information with third party providers.[297]

Cloud computing decreases IT costs and increases overall efficiencies, which has a positive impact on the financial health of corporations.[298] Financially healthy corporations can hire more people, who in turn will have more disposable income to spend, which will benefit the economy. The size of the cloud computing industry, especially if looked at in combination with the energy industry, is significant enough to have an impact on the economy.[299] However, consumers do not want compromised Fourth Amendment rights and will hesitate to convert to a technology where the government has access to the content of their stored electronic communications.[300]

The counter argument to the current administration's position is presented by the Digital Due Process coalition, arguing that Fourth Amendment privacy issues are not sufficiently protected under the ECPA and calling for reform.[301] In particular, the lack of a search warrant requirement, for access to the content of communications stored for more than 180 days, leaves consumer data susceptible to government access.[302] The legal protections have not kept up with technology, and the proposed legislation is a step toward providing Fourth Amendment protection to consumers.[303] As more consum-

295. *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Judiciary Comm.* 3, 5, 6 (2010) (statement of James A. Baker, Assoc. Deputy Att'y Gen. of the U.S. Dep't of Justice), *available at* http://www.justice.gov/ola/testimony/111-2/09-22-10-baker-electronic-comm-privacy-act.pdf; David Kravets, *Justice Dept. to Congress: Don't Saddle 4th Amendment on Us*, WIRED (Apr. 7, 2011, 4:06 PM), http://www.wired.com/threatlevel/2011/04/fourth-amendment-email-2.

296. Kravets, *supra* note 295.

297. *See* Cooke, *supra* note 22, at 3.

298. *See id.*

299. Soghoian, *supra* note 12, at 361.

300. *See* Balough, *supra* note 39, at 103; Cooke, *supra* note 22, at 4; *see also About the Issue*, *supra* note 74.

301. *See Our Principles*, *supra* note 79.

302. *See* Electronic Communications Privacy Act, 18 U.S.C. § 2703(a) (2006 & Supp. III 2009).

303. *See id.* §§ 2–3.

ers are comfortable with storing their private information with third party carriers, the projected growth may be realized.

Unfortunately, the proposed legislation leaves behind smart grid technology.[304] Because of the synergies in telecommunications and energy industries, it is predictable that the same Fourth Amendment issues will arise when smart grid technology is universally deployed.[305] The economy would benefit from the deployment of smart grid—it is estimated that 280,000 jobs will be created.[306] In order for this to occur, consumers will need to feel comfortable with privacy protections.[307] Additionally, the use of smart grid technology would improve the environment.[308] Judicial, government and technical resources would be more efficiently used if both industries were addressed together, and the proposed legislation included a warrant requirement for government access to the content of smart grid information.

Further, in order to address all the Fourth Amendment privacy issues, the current bill should consider how the independent source doctrine and inevitable discovery doctrine might apply to electronic communications. Maybe safeguards aimed at avoiding these exceptions could be incorporated into the proposed legislation. The processable and recoverable characteristics of electronic communications, coupled with remote storage in the cloud, support the circular reasoning of these doctrines. There will be minimal risks to the "search now, warrant later" mentality. Law enforcement agents may be able to get around the search warrant requirement because they will be able to easily meet the threshold inquiries of these doctrines. Consequently, the proposed warrant requirement may be just a futile effort and may be meaningless in certain instances. The proposed legislation might better address Fourth Amendment privacy concerns if it considered the exceptions of the independent source and inevitable discovery doctrines.

304. *See generally* Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011).

305. Balough, *supra* note 39, at 172.

306. *Energy Bar Association Panel Discussing the Smart Grid*, *supra* note 1, at 89.

307. *Id.*

308. *Id.*