NOTE

HEADS IN THE CLOUD, A COMING STORM
THE INTERPLAY OF CLOUD COMPUTING, ENCRYPTION, AND THE FIFTH AMENDMENT'S PROTECTION AGAINST SELF-INCRIMINATION

*David Colarusso**

I. INTRODUCTION

In the past, safes have always been susceptible to the locksmith, and third-party hosts of information, such as banks, to the subpoena. New technologies, however, present law enforcement with the prospect that information may be stored in unknowable locations behind unbreakable locks.[1] A number of legal questions are raised by the migration of personal data to the Internet, and although a great deal of discussion has focused on jurisdiction[2] and Fourth

* J.D. Candidate, Boston University School of Law, Class of 2011; M.Ed., Individualized, Harvard Graduate School of Education, 2002; B.A. Independent Major, Cornell University College of Arts and Sciences, 2001.

[1] *See infra* Parts III, IV.

[2] *See, e.g.*, Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001); Gwenn M. Kalow, Note, *From*

Amendment[3] considerations, little has been written about the Fifth Amendment implications presented by such a migration.[4] This is not the case for the more generic migration of personal data from physical to digital media where the use of encryption software restricts access to data, often requiring the production of a password or phrase, implicating the Fifth Amendment's protection against self-incrimination.[5] The testimonial nature of such a production remains an

the Internet to Court: Exercising Jurisdiction over World Wide Web Communications, 65 FORDHAM L. REV. 2241 (1997); Todd D. Leitstein, Comment, *A Solution for Personal Jurisdiction on the Internet*, 59 LA. L. REV. 565 (1999); Nathan A. Olin, *The A-B-Cs of Targeting: A Formula for Resolving Personal Jurisdiction-Internet Issues within the District of Massachusetts*, 23 W. NEW ENG. L. REV. 237 (2002); Joel R. Reindenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951 (2004-2005); David Wille, *Personal Jurisdiction and the Internet Proposed Limits on State Jurisdiction over Data Communications in Tort Cases*, 87 KY. L.J. 95 (1999); Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet*, 50 FED. COMM. L.J. 117 (1997-1998); Richard S. Zembek, Comment, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L.J. SCI. & TECH. 339 (1996).

[3] *See, e.g.*, Johnny Gilman, Comment, *Carnivore: The Uneasy Relationship between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111 (2001); Matthew J. Hodge, Comment, *The Fourth Amendment and Privacy Issues on the New Internet: Facebook.com and Myspace.com*, 31 S. ILL. U. L.J. 95 (2006); David Alan Jordan, *Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice over Internet Protocol*, 47 B.C. L. REV. 505 (2006); Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591 (1997); Matthew D. Lawless, Note, *The Third Party Doctrine Redux: Internet Search Records and the case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 2 (2007); Amy E. Wells, Comment, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99 (2000).

[4] For example, as of April 3, 2010, a Westlaw title search of journals and law reviews for the pairing of "Fifth Amendment" and any combination of "world wide web," "cloud computing," "Internet," or "network" returns a single result. *See* Wendy Perdue, *Aliens, the Internet, and "Purposeful Availment": A Reassessment of Fifth Amendment Limits on Personal Jurisdiction*, 98 NW. U. L. REV. 455 (2004). Additionally, this article examines due process under the Fifth Amendment whereas this paper focuses on the Fifth Amendment right against self-incrimination.

[5] *See, e.g.*, Aaron M. Clemens, Note, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, 2004 UCLA J.L. & TECH. 2 (2004); Lance Cole, *The Fifth Amendment and Compelled Production of Personal Documents After United States v. Hubbell - New Protection for Private Papers?*, 29 AM. J. CRIM. L. 123, 166 (2002); Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (1996); David B. Walker, *Privacy in the Digital Age: Encryption Policy –A Call for Congressional Action*,

open question of law and so too the extent to which it may be protected by the Fifth Amendment's prohibition on self-incrimination. Currently, a handful of cases addressing this issue are working their way through the federal courts.[6] However, even after these questions are resolved, the consequences of strong encryption upon Fifth Amendment jurisprudence will loom large over the migration of data to what is coming commonly to be known as "the cloud."[7]

In July 2009, Google announced plans to launch Google Chrome OS, an "attempt to re-think what the operating system should be."[8] Growing out of Google's Chrome browser, the operating system promises to present a web-centered user experience in which the "web is the platform."[9] Chrome OS is one in a long line of web-based applications commonly referred to as "cloud computing"[10] in which the bulk of data storage and processing takes place on the network, not on the user's computer.[11] The implications of maintaining and interacting with data in such a manner are far reaching, spanning the practical[12] and the legal.[13] The development of cloud computing is part of the

1999 Stan. Tech. L. Rev. 3 (1999); Andrew J. Ungberg, Note, *Protecting Privacy through a Responsible Decryption Policy*, 22 Harv. J. L. & Tech. 537 (2009).

[6] *See* U.S. v. Gavegnano, 305 Fed. Appx. 954 (4th Cir. 2009); U.S. v. Kirschner, No. 09-MC-50872, 2010 WL 1257355 (D. Mich. March 30, 2010); *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[7] *See infra* Part V.C.

[8] Sundar Pichai, *Introducing the Google Chrome OS*, Official Google Blog (Jul. 7, 2009, 9:37 AM), http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.html.

[9] *Id.*

[10] Google offers a number of these services, including Gmail, Picasa, and Google Docs. *See* Brian Hayes, *Cloud Computing*, Communications of the ACM, Jul. 2008 at 9, 9.

[11] The "cloud" in "cloud computing" derives from computer engineers' use of the cloud as a metaphor for the network, as it often showed up in design specifications as a cartoon cloud. Its usage is analogous to the general engineering usage of "black box." *See* Jessie Holliday Scanlon and Brad Wieners, *Guest Column: The Internet Cloud*, Computerworld (Jul. 16, 1999), http://www.computerworld.com.au/article/104942/guest_column_internet_cloud/.

[12] Storing information in the cloud allows it to be accessed from more than one networked device, allowing its author to access and share documents in novel ways. *See* Google, *Google Docs In Plain English*, YouTube (Sep. 10, 2007), http://www.youtube.com/watch?v=eRqUE6IHTEA. However, this also places a great deal of trust in the curator of the cloud, opening users up to potential data loss at the hands of their service provider. *See* Rob Pegoraro, *Flash Forward: Sidekick Users See Their Data Vanish Into a Cloud*, Wash. Post (Oct. 13, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/10/12/AR2009101203012.html.

[13] *See, e.g.*, R. Bruce Wells, Comment, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, 12 U. Pa. J. Const. L. 223 (2009).

larger growth of computer technology, which as a whole has stressed traditional legal principles by prompting their application to facts unforeseen at the time of their drafting.[14] Many of the legal implications presented by these stressors have been examined, especially in relation to matters of jurisdiction and privacy.[15] However, only recently has the Fifth Amendment's self-incrimination clause found itself clearly implicated in this changing landscape.[16] In 2007, Sebastien Boucher invoked his Fifth Amendment right against self-incrimination in refusing to produce a password that the government needed in order to decrypt and examine the contents of his laptop.[17] Boucher maintained that to produce the password, he would have to reveal "the contents of his mind" in violation of his Fifth Amendment right, and a federal magistrate agreed.[18] In February 2009, however, the United States District Court for the District of Vermont ordered Boucher to produce the password, reasoning that the contents of his laptop were a foregone conclusion as a portion of them had been viewed by a border guard prior to the laptop's confiscation.[19] Boucher has signaled his intent to appeal.[20] In March of 2010, under a similar factual pattern, the United States District Court for the Eastern District of Michigan found the production of a password testimonial.[21] We may be seeing the start of a circuit split. Given the rise of cloud computing,[22] it seems likely that similar questions surrounding the interaction of the Fifth Amendment and cloud computing are imminent. As more data is stored in the cloud, access to data is about more than the ability to read it as in *Boucher II*. In the world of cloud computing, an individual's files are stored

[14] *See supra* notes 2-5.

[15] *See supra* notes 2 & 3.

[16] *In re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

[17] *Id*. at *1.

[18] *Id*. at *4, *6.

[19] *In re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *3-4 (D. Vt. Feb. 19, 2009).

[20] Julian Sanchez, *Court: Self-incrimination Privilege Won't Protect Password*, ARS TECHNICA (Mar. 2, 2009, 9:30 AM), http://arstechnica.com/tech-policy/news/2009/03/court-self-incrimination-privilege-stops-with-passwords.ars.

[21] *Kirschner*, 2010 WL 1257355, at *4.

[22] "Industry analysts have made bullish projections on how Cloud computing will transform the entire computing industry. According to a recent Merrill Lynch research note, Cloud computing is expected to be a '$160-billion addressable market opportunity, including $95-billion in business and productivity applications, and another $65-billion in online advertising'. Another research study by Morgan Stanley has also identified Cloud computing as one of the prominent technology trends." Rajkumar Buyya et al., *Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility*, 25 FUTURE GENERATION COMPUTER SYSTEMS 6, 599, 606 (2009) (footnotes omitted).

almost exclusively in the cloud, not to be found on any desktop or laptop hard drive. Consequently, one must know more than a password to read files; one must know where they are located. If the data's location is truly unknown to law enforcement, such a scenario presents a practical problem just as insoluble as that of the nearly unbreakable codes produced by strong encryption and present in *Boucher I*, requiring that the accused communicate the contents of his mind in order for law enforcement to gain access to his files.[23] This matter is further complicated when encryption is coupled with storage in the cloud and users make use of anonymous Internet access, precluding the cooperation of service providers in establishing a user's identity. Together these changes in how information is stored and accessed present a coming storm for law enforcement.

Part II below examines the current state of Fifth Amendment jurisprudence surrounding the privilege of production, while parts III and IV present brief technical overviews of data encryption and cloud computing respectively. Part V examines the Fifth Amendment implications of encryption and cloud computing, first separately, and then collectively. Part VI further explores the implications of such pairings and outlines four options available to the government and law enforcement in response to the issues raised. Finally, the desirability of these options are examined under the shadow of likely future scientific developments.

II. THE ACT OF PRODUCTION

The Fifth Amendment's prohibition on self-incrimination protects one against the compelled communication of incriminating testimonial information.[24] It does not protect the informational content of objects or identifying attributes such as personal documents,[25] blood samples,[26] handwriting,[27] signatures,[28] or the sound of one's voice.[29] Rather, it prohibits one from being compelled to share the incriminating "contents of [one's] own mind."[30] Consequently, it may protect only the production of some physical thing when the production of that thing communicates some incriminating information, such as the confirmation of its existence, the implicit or explicit admission of control over it, or its authentication.[31] The fact that the thing in

[23] *See Boucher I*, 2007 WL 4246473, at *4, *6.

[24] *See* Fisher v. United States, 425 U.S. 391, 409 (1976).

[25] *See id.* at 408-09.

[26] *See* Schmerber v. California, 384 U.S. 757, 761, 765 (1966).

[27] *See* Gilbert v. California, 388 U.S. 263, 266-67 (1967).

[28] *See* Doe v. United States, 487 U.S. 201, 217-18 (1988).

[29] *See* United States v. Wade, 388 U.S. 218, 222-23 (1967).

[30] Curcio v. United States, 354 U.S. 118, 128 (1957).

[31] *See* United States v. Hubbell, 530 U.S. 27, 45 (2000).

question may incriminate an individual is insufficient to imbue it with protection.[32] As the Supreme Court recognized in *United States v. Hubbell*:

> The term "privilege against self-incrimination" is not an entirely accurate description of a person's constitutional protection against being "compelled in any criminal case to be a witness against himself."
>
> The word "witness" in the constitutional text limits the relevant category of compelled incriminating communications to those that are "testimonial" in character. As Justice Holmes observed, there is a significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating.[33]

In *Hubbell*, the defendant entered into a plea bargain with the Independent Counsel assigned to investigate possible violations of federal law related to the Whitewater Development Corporation.[34] The defendant pled guilty to mail fraud and tax evasion.[35] Additionally, he "promised to provide the Independent Counsel with 'full, complete, accurate, and truthful information' about matters relating to the Whitewater investigation."[36] In an attempt to ascertain whether or not the defendant had complied with this promise, the Independent Counsel served the defendant with a subpoena *duces tecum* calling for the production of any documents he might possess which fell into any of eleven classes described in the subpoena.[37] The defendant invoked his Fifth Amendment right against self-incrimination, and "[i]n response to questioning by the prosecutor, respondent initially refused 'to state whether there are documents within [his] possession, custody, or control responsive to the Subpoena.'"[38] Eventually, however, the defendant was directed to respond to the subpoena and was granted immunity "to the extent allowed by law."[39] Subsequently, the defendant produced 13,120 pages of documents relating to the classes laid out in the subpoena.[40] Using information found in these documents, the Independent Counsel initiated a second prosecution against the defendant, indicting him on a number of tax crimes along with wire and mail fraud.[41] Given that "the Independent Counsel had admitted that he was not

[32] *See id*. at 35.

[33] *Id*. at 34-35 (citations omitted).

[34] *Id*. at 30.

[35] *Id*.

[36] *Id*. (citation omitted).

[37] United States v. Hubbell, 530 U.S. 27, 31 (2000).

[38] *Id*. (citation omitted).

[39] *Id*. (citation omitted).

[40] *Id*.

[41] *Id*.

investigating tax-related issues when he issued the subpoena, and that he had learned about the unreported income and other crimes from studying the records' contents, the District Court characterized the subpoena as "the quintessential fishing expedition."[42] The Supreme Court agreed with the District Court, holding the defendant's production to be privileged.[43]

> What the District Court characterized as a "fishing expedition" did produce a fish, but not the one that the Independent Counsel expected to hook. It is abundantly clear that the testimonial aspect of respondent's act of producing subpoenaed documents was the first step in a chain of evidence that led to this prosecution. The documents did not magically appear in the prosecutor's office like "manna from heaven." They arrived there only after respondent asserted his constitutional privilege, received a grant of immunity, and—under the compulsion of the District Court's order—took the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the many sources of potentially incriminating evidence sought by the subpoena. It was only through respondent's truthful reply to the subpoena that the Government received the incriminating documents of which it made "substantial use . . . in the investigation that led to the indictment."
>
> . . . .
>
> In sum, we have no doubt that the constitutional privilege against self-incrimination protects the target of a grand jury investigation from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence. That constitutional privilege has the same application to the testimonial aspect of a response to a subpoena seeking discovery of those sources.[44]

This privilege, however, does not exist when the information communicated by a production constitutes a "foregone conclusion."[45] In *Fisher v. United States*, the government sought to obtain work papers prepared by the defendant's accountant.[46] The government was already aware of the existence and nature of these documents, and in rejecting the defendant's claim of privilege, the Supreme Court observed:

> It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment. The papers belong to the accountant, were prepared by him, and are the kind usually prepared by an accountant working on

[42] *Id*. at 32 (internal quotation marks and citation omitted).

[43] United States v. Hubbell, 530 U.S. 27 (2000).

[44] *Id*. at 42-43 (citation omitted).

[45] *Id*. at 44 (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).

[46] *Fisher*, 425 U.S. at 411.

> the tax returns of his client. Surely the Government is in no way relying on the "truthtelling" of the taxpayer to prove the existence of or his access to the documents. The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender."[47]

According to *Fisher*, there are three instances in which production may be privileged: (1) when it confirms the existence of evidence; (2) when it confirms control or possession over evidence; or (3) when it authenticates evidence.[48] A similar situation to *Fisher*'s foregone conclusion is present in cases involving the production of body products and identifying attributes such as blood samples, writing samples, and voice recordings since the existence and control of these is not in question.[49]

In *Doe v. United States*, the defendant was the subject of a federal grand jury investigation of possible federal offenses relating to unreported income and the fraudulent manipulation of oil cargo.[50] The government issued a subpoena directing Doe to produce records relating to bank accounts in the Cayman Islands and Bermuda that it suspected to be under his control.[51] Doe produced some records, but when asked about the existence of additional accounts, he invoked his Fifth Amendment privilege against self-incrimination.[52] The government also served subpoenas to several U.S. branches of these banks.[53] Citing the securities laws governing their banks' operation, the banks declined cooperation without first receiving the customer's consent.[54] Consequently, the government presented Doe with a consent form framed in the hypothetical that authorized the release of any information relating to any accounts for which Doe was authorized to sign a release.[55] Describing the arrangement, the Court had this to say:

> The consent directive itself is not "testimonial." It is carefully drafted not to make reference to a specific account, but only to speak in the hypothetical. Thus, the form does not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by

[47] *Id.* (citations omitted).

[48] *Id.* at 408, 410-13.

[49] *See* Pennsylvania v. Muniz, 496 U. S. 582, 594-98 (1990).

[50] Doe v. United States, 487 U.S. 201, 202 (1988).

[51] *Id.* at 202-203.

[52] *Id.* at 203.

[53] *Id.*

[54] *Id.*

[55] Doe v. United States, 487 U.S. 201, 204 (1988).

> petitioner. Nor does the form indicate whether documents or any other information relating to petitioner are present at the foreign bank, assuming that such an account does exist. The form does not even identify the relevant bank. Although the executed form allows the Government access to a potential source of evidence, the directive itself does not point the Government toward hidden accounts or otherwise provide information that will assist the prosecution in uncovering evidence. The Government must locate that evidence " 'by the independent labor of its officers,' " As in *Fisher*, the Government is not relying upon the " 'truth-telling' " of Doe's directive to show the existence of, or his control over, foreign bank account records.[56]

That is, the Court "read the directive as equivalent to a statement by Doe that, although he expresses no opinion about the existence of, or his control over, any such account, he is authorizing the bank to disclose information relating to accounts over which, in the bank's opinion, Doe can exercise the right of withdrawal."[57] In this way, Doe avoids making a testimonial statement in which the existence, control, or authentication of the documents is established and so avoids implicating his Fifth Amendment privilege against self-incrimination.

This nuanced jurisprudential interpretation of the Fifth Amendment's self-incrimination clause is a far departure from that present in the early half of the twentieth century and exemplified by *Boyd v. United States*.[58] In *Boyd* a unanimous Court held that the Fifth Amendment protected individuals from the forced production of books and papers.[59] The Court's current stance is likely a response to the government's growing interest in white-collar crime and the need for access to working papers.[60] It remains to be seen, however, how the Court will respond to the pressures presented by new technologies which present the possibility that information may be stored in unknowable locations behind unbreakable locks.[61]

III. Encryption

Encryption is the process of obscuring meaning through a deliberate and reversible transformation, and there is evidence of its practice dating back nearly four millennia.[62] Consequently, the American legal system has

[56] *Id*. at 215.

[57] *Id*. at 217-18.

[58] Boyd v. United States, 116 U.S. 616 (1886).

[59] *Id*. at 638-39.

[60] William J. Stuntz, Commentary, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 859-60 (2001).

[61] *See infra* Parts V, VI.

[62] Network Associates, Inc., *How PGP Works*, THE INTERNATIONAL PCP HOMEPAGE, 11,

encountered its use since the early days of the republic.[63] Modern innovations, however, have resulted in the creation of encryption schemes so difficult to break that practical considerations render them effectively unbreakable.[64] Given the power of today's computers, it could take longer to break such encryption than there are years left in the universe.[65]

A. Symmetric Key Encryption

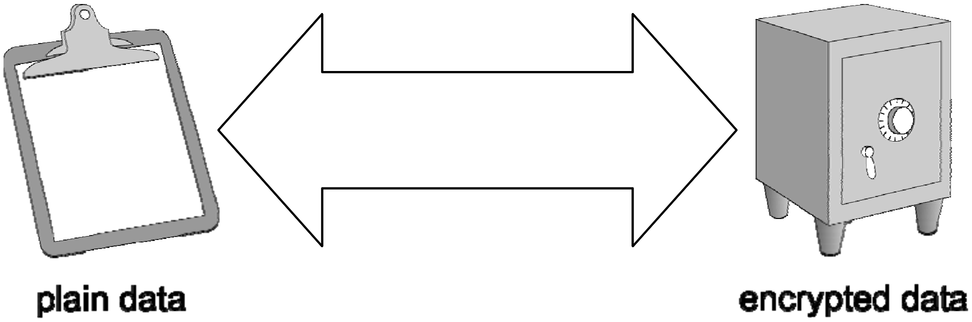

Figure 1: Conventional (symmetric key) Encryption makes use of a key and cipher to encrypt plaintext and decrypt ciphertext.[66]

Conventional encryption, also known as symmetric key encryption, takes generally intelligible information, known as plaintext, and obscures its meaning, transforming it into "unreadable gibberish," known as ciphertext.[67] This is done according to the application of a cipher, a set of rules that describes how to transform the plaintext.[68] The cipher is an algorithm that takes in both the plaintext and a key—such as a word, phrase, or number.[69] The key is used as a seed around which to build the ciphertext, different keys resulting in different outputs.[70] The effectiveness of such encryption is dependent upon both the strength of the cipher and the secrecy of the key.[71]

ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf (last visited October 19, 2010).

[63] United States v. Burr (*In re* Willie), 25 F. Cas. 38, 39 (C.C.D. Va. 1807).

[64] Network Associates, Inc., *supra* note 62 at 12.

[65] *Id.*

[66] Image inspired by PGP documentation Figure 1-2. Network Associates, Inc., *supra* note 62 at 11.

[67] Network Associates, Inc., *supra* note 62 at 11.

[68] *Id.* at 12.

[69] *Id.*

[70] *Id.*

[71] *Id.*

The Caesar cipher is one of the oldest and most widely known examples of encryption.[72] Used by Julius Caesar to communicate with his generals, the Caesar cipher simply shifts the letters of the alphabet, for example, replacing A with E, B with F, and so on.[73] Here the key is the number four, the amount by which one shifts the alphabet, and the cipher is the shifting rule itself. Generally, the larger the number of possible keys, the stronger the encryption since decryption via brute force (trying all possible keys) will on average require a greater number of attempts. Conventional encryption schemes require both the author and recipient to possess a copy of the cipher and key, meaning they are both able to encrypt and decrypt the message. This presents a problem, however, for one cannot use such a scheme to secretly communicate with someone without first secretly sharing either the cipher or the key. Consequently, the sharing of secret information between previously unacquainted/unconnected parties requires an alternate solution.

B. Public Key Encryption

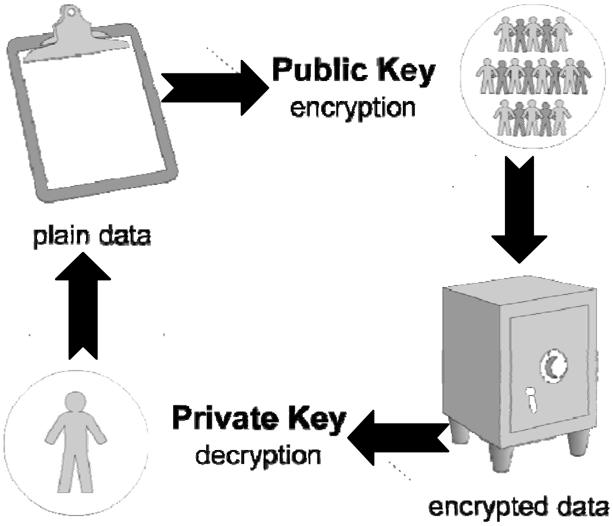

Figure 2: Public Key Encryption makes use of a public key to encrypt plaintext and a private key to decrypt ciphertext.[74]

This problem of previously unacquainted/unconnected parties is solved by the use of *public key cryptography* wherein one key is used to encrypt data and

[72] *Id*. at 13.

[73] Network Associates, Inc., *supra* note 62 at 13-14.

[74] Image inspired by PGP documentation Figure 1-3 Network Associates, Inc., *supra* note 62, at 15.

another is used to decrypt it.[75] The former, a public key, can be widely distributed along with the cipher, and the latter, a private key, can be kept secret by the intended recipient of the ciphertext.[76] Such keys are constructed from the pairing of two large randomly-generated prime numbers.[77] The original prime numbers constitute the private key, and their product is used as the public key.[78] Given the two primes, making this public key is easy. One simply multiplies the two numbers. However, if one is given only the public key, finding the two primes is considerably more difficult. That is, multiplication is easy; factoring is hard. Public key ciphers take advantage of this difference in difficulty.[79] Although it is theoretically possible to discover the private key given the public key, the difficulty involved is so great as to render it impractical.[80] The exact manner in which this one-way difference in difficulty is exploited is unimportant for our purposes. It is enough to know that the difficulty is related to the size of the numbers involved and that for sufficiently large numbers, the task of decryption via brute force is hard enough as to potentially take billions of years or billions of computers given current computing power.[81]

Commonly available encryption software such as Pretty Good Privacy (PGP), the software used to encrypt Broucher's Z Drive,[82] makes use of both conventional and public key encryption to protect communication over the Internet,[83] using at least three keys: a conventional key memorized by the user in the form of a password or passphrase and a public-private key pairing, which the user does not memorize. The conventional key is used to encrypt the user's private key, which is stored locally on the user's computer.[84] Consequently, a user must enter her conventional key in order to decrypt her private key, which is then used to decrypt communications encrypted by her public key.[85] The public key encryption protects against individuals who might intercept the communication, whereas the conventional key encryption of the private key protects against unauthorized access to the user's computer.

[75] R. L. Rivest, A. Shamir & L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 COMMUNICATIONS OF THE ACM 120 (1978).

[76] *Id*. at 120-22.

[77] *Id*. at 122-24.

[78] *Id*. at 122-23.

[79] *Id*. at 122-25.

[80] *Id*. at 125.

[81] Network Associates, Inc., *supra* note 62 at 12.

[82] *In Re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *2 (D. Vt. Nov. 29, 2007).

[83] Network Associates, Inc., *supra* note 62 at 16.

[84] *Id*.

[85] *Id*. at 17.

When two-way communication is required, both users first exchange public keys allowing them to encrypt their respective communications.

IV. CLOUD COMPUTING

A. Today's Weather

Like its namesake, the precise definition of cloud computing remains somewhat fuzzy around the edges,[86] having only entered common usage in late 2007.[87] Among the many disparate definitions, however, there exists a general recognition that cloud computing is the practice of storing and processing data apart from the local machines on which users access it.[88] Such an arrangement is nothing new as "[s]imilar scenario[s] occurred around 50 years ago: [with] time-sharing computing server[s] serv[ing] multiple users."[89] In fact, until the advent of the personal computer, most data was stored and processed by such centralized resources.[90] This, however, is not to say that cloud computing is a "recurrence of [this] history." [91] Mid- twentieth century centralization was driven by the scarcity of computing resources whereas the current motion towards cloud computing often derives from users' need "to handle complex IT infrastructures."[92] Additionally, the nature of the data stored in the cloud today differs from that found on networks fifty years ago. Such networks predated the personal computer and were primarily the hosts of data belonging to large companies, universities, and the government. Today, however, three billion personal photographs are uploaded to Facebook every month.[93] Shifting data storage and processing to the cloud offers the end-user and infrastructure manager a number of benefits, from web-accessible content control to on-demand scalable resources.[94] Most relevant to this note's legal

[86] Ian Foster, Yong Zhao, Ioan Raicu & Shiyong Lu, *Cloud Computing and Grid Computing 360-Degree Compared*, GRID COMPUTING ENVIRONMENTS WORKSHOP, 2008. GCE '08, November 2008, at 1, 1; Lizhe Wang et al., *Scientific Cloud Computing: Early Definition and Experience*, PROC. OF THE 10TH IEEE INT'L CONF. ON HIGH PERFORMANCE COMPUTING AND COMM., October 26, 2008 at 825, 825 (2008); Luis M. Vaquero et al., *A Break in the Clouds: Towards a Cloud Definition*, 39 ACM SIGCOMM COMPUTER COMMUNICATION REVIEW, January 2009, at 50, 50.

[87] Wang, *supra* note 86, at 825.

[88] Vaquero, *supra* note 86, at 50. *See also* Wang, *supra* note 86, at 825-28.

[89] Wang, *supra* note 86, at 3.

[90] *Id*.

[91] *Id*.

[92] *Id*.

[93] *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited March 5, 2010).

[94] Wang, *supra* note 86, at 827-28.

considerations, however, is that cloud computing offers users the ability "to access applications from anywhere in the world on demand."[95]

> Whether it's called cloud computing or on-demand computing, software as a service, or the Internet as platform, the common element is a shift in the geography of computation. When you create a spreadsheet with the Google Docs service, major components of the software reside on unseen computers, whereabouts unknown, possibly scattered across continents.[96]

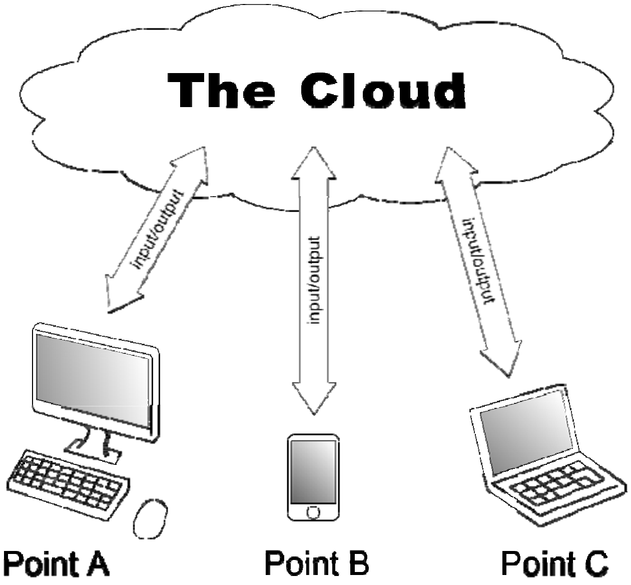

Figure 3: By storing and manipulating data in remote datacenters, users can place their data in "the cloud," allowing access from multiple devices.

The metaphor of "the cloud" serves as a place holder to describe the centralized network space in which data is stored and processed, the name deriving from the practice of placing this space in a cartoon cloud when sketching out the components of a service.[97] Since a user's data is stored in "the cloud," it is not anchored to any one device or location. A user can just as easily access her data from Points A, B, or C. Likewise, an individual can share data with collaborators who have access to the cloud. Assuming that the

[95] Rajkumar, *supra* note 22, at 599.

[96] Hayes, *supra* note 10, at 9.

[97] *See* Scanlon, *supra* note 11.

user trusts the curators of her data, she need not even maintain a local copy.[98] In addition to being email systems, web-based services such as Hotmail, Yahoo! Mail, and Gmail are also high-profile examples of cloud computing, storing massive amounts of user data in "the cloud" on servers across the globe. Users may access their emails from their home computer, web-enabled phone, laptop, or even a public workstation at an internet café or library.

B. The Extended Forecast

Google Chrome OS envisions a "lightweight operating system" where "the web is the platform," effectively moving many traditional computing services into the cloud along with user data.[99] Google is already offering a number of cloud-based applications, including Gmail and the Google Docs suite. "The kinds of productivity applications that first attracted people to personal computers 30 years ago are now appearing as [cloud computing applications]. The Google Docs programs are an example, including a word processor, a spreadsheet, and a tool for creating PowerPoint-like presentations."[100] Google, however, does not have a monopoly on this migration of services to the cloud.[101] "According to a recent Merrill Lynch research note, Cloud computing is expected to be a '$160-billion addressable market opportunity . . . ' "[102] and "[g]overnments, research institutes, and industry leaders are rushing to adopt Cloud Computing to solve their ever-increasing computing and storage problems arising in the Internet Age."[103] The Obama administration signaled its interest in cloud computing, highlighting the technology in its 2010 budget request,[104] and in September the General Services Administration launched a cloud storefront, Apps.gov, intended to "enhanc[e] how the government leverages technology by enabling federal agencies to acquire and purchase cloud computing services in an efficient, effective manner."[105] Coinciding with this announcement, Google announced the creation of a government cloud, "which [Google] expect[ed] to become operational in 2010. Offering the same services and features as [Google's] existing commercial

[98] As noted earlier, however, this can be a risky proposition. *See* Pegoraro, *supra* note 12.

[99] Pichai, *supra* note 8.

[100] *See* Hayes, *supra* note 10, at 10.

[101] *See* Rajkumar, *supra* note 22, at 606.

[102] *Id*.

[103] Foster, *supra* note 86, at 1.

[104] Doug Beizer, *FAQ: Obama's cloud initiative*, FEDERAL COMPUTER WEEK (May 15, 2009), http://www.fcw.com/Articles/2009/05/18/NEWS-Obama-in-the-cloud.aspx.

[105] Caren Auchman, *Obama Administration Launches GSA Cloud Storefront Apps.gov*, US GENERAL SERVICES ADMINISTRATION (Sept. 15, 2009), http://www.gsa.gov/portal/content/103758.

cloud (such as Google Apps), this dedicated environment within existing Google facilities in the U.S. will serve the unique needs of U.S. federal, state, and local governments. It is similar to a 'Community Cloud' as defined by the National Institute for Science and Technology."[106] Even the U.S. Department of Defense is on board, running an Apps for Army competition, in which it encourages its soldiers to produce open source software for the benefit of DoD, to be hosted in the Department's own secure cloud—forge.mil.[107] Former Nokia CTO Bob Iannucci has said that he sees the future of mobile phones in the cloud,[108] a direction apparently embraced by mobile provider AT&T given its recent announcement of a new set of cloud-based services.[109] Allan Knies, associate director of Intel Research Berkeley, has even proposed placing cloned copies of mobile phones in the cloud,[110] and many in the tech community are characterizing Apple's iPad as the latest escalation in the battle between Google and Apple over who will dominate the cloud.[111] As bandwidth increases and the barriers to access crumble, the cloud's role as the repository of our data seems endless.[112]

[106] Matthew Glotzbach, *Google Apps and Government*, OFFICIAL GOOGLE ENTERPRISE BLOG (Sept. 15, 2009, 11:45 AM), http://googleenterprise.blogspot.com/2009/09/google-apps-and-government.html.

[107] J. Nicholas Hoover, *Gov 2.0: Army Announces Apps For Army Competition*, INFORMATIONWEEK GOVERNMENT (Sept. 10, 2009, 4:17 PM), http://www.informationweek.com/news/government/enterprise-apps/showArticle.jhtml?articleID=219700596.

[108] Stephen Lawson, *Future of mobile phones is in the cloud, ex-Nokia CTO says*, INFOWORLD (Apr. 16, 2009), http://www.infoworld.com/d/mobilize/future-mobile-phones-in-cloud-ex-nokia-cto-says-721.

[109] Bonnie Cha, *AT&T unleashes new messaging phones and cloud services*, DIALED IN - CCET BLOGS (March 15, 2010), http://www.cnet.com/8301-17918_1-20000427-85.html.

[110] Christopher Mims, *Sending Cell Phones into the Cloud*, TECHNOLOGY REVIEW (May 1, 2010) http://www.technologyreview.com/communications/22571/.

[111] *See, e.g.*, Robert Licursi, *The Gloves Are Off: Chromium OS Netbooks vs. The iPad for Cloud Computing*, EXAMINER.COM (Jan. 30, 2010, 7:51 PM), http://www.examiner.com/x-33449-Chicago-Cloud-Computing-Examiner~y2010m1d30-The-Gloves-Are-Off--Chromium-OS-Netbooks-vs-The-iPad-for-Cloud-Computing; CJ: Christine, *Apple Ipad vs Chrome? Cloud computing war may occur*, MERINEWS (Jan. 31, 2010, 3:58 AM), http://www.merinews.com/article/apple-ipad-vs-chrome-cloud-computing-war-may-occur/15796261.shtml; Clint Boulton, *Apple iPad Challenges Google's Chrome Cloud Computing Designs*, EWEEK.COM (Jan. 30, 2010), http://www.eweek.com/c/a/Cloud-Computing/Apple-iPad-Challenges-Googles-Chrome-Cloud-Computing-Designs-219397/.

[112] Laurie Sullivan, *Google's Ultra-High-Speed Fiber Network Will Boost Cloud Computing*, MEDIAPOST (March 8, 2010, 3:00 PM), http://www.mediapost.com/?fa=Articles.showArticle&art_aid=123846.

V. FIFTH AMENDMENT IMPLICATIONS

A. Encryption

The Supreme Court has repeatedly distinguished between the testimonial nature of a key and that of the combination to a safe, suggesting that the latter is privileged as in *Doe v. U.S.*[113] This construction has led many to assume that the production of a password from memory is an "expression of the contents of an individual's mind" and therefore privileged under the act of production.[114] In *Hubbell* this analogy was used to illustrate the testimonial nature of the defendant's production. "It was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena. The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[115] *In re Boucher* has brought this question of a password's testimonial nature to the fore, and the ultimate outcome is not yet clear.[116] The Court's reliance on *Fisher* and its "foregone conclusion" rationale sidesteps the question as to the testimonial nature of passwords *per se*.[117] Had the border guard not seen the contents of Boucher's computer, there would be little or no obvious assertion that the contents were a foregone conclusion.[118]

Additionally, it may not be prudent to so closely analogize encryption keys to safe combinations given that non-privileged biometric data can be used in the place of a password.[119] Should the protection afforded encrypted files depend on this choice of encryption keys? What would justify such a distinction? Then again, what justifies the distinction between a combination and a physical key held in an unknown location? Doesn't the production of such a key reveal the contents of one's mind and establish at least existence, control, or authentication? The reasoning in *Boucher II* presents a potential

[113] *See e.g.*, United States v. Hubbell, 530 U.S. 27, 34-36 (2000); Doe v. United States, 487 U.S. 201, 210 n.9 (1988).

[114] Doe v. United States, 487 U.S. 201, 210 n.9 (1988); *See e.g.*, Clemens, *supra* note 5, at 24-27; Adam C. Bonin, Comment, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL. F. 495, 514 (1996).

[115] United States v. Hubbell, 530 U.S. 27, 43 (2000) (citations omitted).

[116] *Compare Kirschner*, 2010 WL 1257355 (accepting the production of a password as testimonial), and *Boucher II*, 2009 WL 424718 (rejecting the production of a password as testimonial).

[117] *In Re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009).

[118] *In Re* Boucher (*Boucher I*), No. 2:06-mj-91, 2007 WL 4246473, at *5 (D. Vt. Nov. 29, 2007), at *5; Ungberg, *supra* note 5, at 539.

[119] Ungberg, *supra* note 5, at 547-48.

argument for the unprotected production of any encryption key/password linked to files stored on media within the state's possession regardless of the *per se* nature of passwords, be they testimonial or not. It may be true that "[t]he government can compel message decryption or private key production only where it proves that the requested document or private key: (1) exists; (2) was possessed, located or controlled by the person it is requested from; and (3) will not have its authentication assisted by this decryption or production."[120] However, the fact that a personal computer is under the control of its owner may negate these points. Phillip R. Reitinger, former DOJ trial lawyer, Computer Crime and Intellectual Property Section, anticipated such an argument in the mid-nineties, suggesting that the combination-key distinction is a false dichotomy, "That I physically lock that document in a safe is not material; so long as the document is in my custody, I must produce it in response to a legally authorized demand. The result should not differ if, instead of locking the document in a safe, I lock the contents through encryption . . . even if I store the document on a computer that requires a password for access, I must produce the document when faced with an authorized demand. Similarly, if I encrypt the document, I should be required to produce the unencrypted version if I receive an authorized demand for the same."[121] Put another way, if the computer was under the control of the accused, so too were its contents. Consequently, the production of such cannot be testimonial. This is the sentiment echoed in *Boucher II*,[122] and it establishes a clear path for courts to declare passwords non-testimonial in many cases, avoiding the need to rule on the *per se* nature of passwords.

To see how a court could make use of such an argument, imagine a scenario in which a computer is confiscated as part of the legal search of a residence. The contents of the computer are encrypted, and it is established that no one other than the accused has had access to the computer since its purchase.[123] It is clear that the computer contains information although the content of that information is unknown, yet the contents of the computer are clearly covered by the search warrant. There is no question that files exist, and it is not a

[120] Clemens, *supra* note 5, at 12. *See* Cole *supra* note 5, at 166.

[121] Reitinger, *supra* note 5, at 176.

[122] *In Re* Boucher (*Boucher II*), No. 2:06-mj-91, 2009 WL 424718, at *3 (D. Vt. Feb. 19, 2009) ("[P]roviding access to the unencrypted Z drive 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information.") (quoting Fisher v. US, 425 U.S. 391, 411 (1976)).

[123] We are taking the accused's exclusive control as a given. However, it is interesting to note that physical control over a networked computer does not necessarily imply control over its contents. *See* Robert McMillan, *Guilty Verdict Dropped in Porn Pop-Up Case Against Teacher*, PC WORLD (Jun. 6, 2007, 5:00 PM) http://www.pcworld.com/article/132629/guilty_verdict_dropped_in_porn_popup_case_against_teacher.html.

stretch to conclude that the accused's control over these files is a foregone conclusion. Given a broad reading of *Fisher* as articulated in *Boucher II*, the password is not privileged for there is no question as to the existence, control, and authentic nature of the files.

Additionally, law enforcement seeking to gain access to encrypted files could immunize the accused to avoid privilege.[124] "An assertion of the privilege against self-incrimination is nullified where the government provides use and derivative-use immunity. This immunity removes any danger of prosecution due to the person's compelled testimony. Therefore, such a grant of immunity is 'coextensive with the scope of the privilege against self-incrimination.'"[125] As in *Hubbell*, the product of such an immunized production may not yield the results desired by law enforcement. However, the crafting of immunities designed to address the particular concerns presented by encryption may present law enforcement with a partial alternative to the reasoning in *Boucher II* should it be overturned or in those cases where the data sought is not a foregone conclusion.[126]

B. Cloud Computing

To understand how the Fifth Amendment interacts with cloud computing, let us build upon the example above, pausing along the way to consider potential roadblocks as they arise. A computer is seized as part of a legal residential search. The contents of this computer, however, are not encrypted, and it is running a web-centric operating system (OS) such as Google Chrome. It is clear from log files present on the computer that the user makes use of cloud-based file storage. A web-browser's Internet history and cookies are potentially familiar examples of such files.[127] If these local files make it clear where the cloud-based files are stored, presumably, the government could easily obtain a subpoena for their production, aimed at the cloud computing service itself. Such a subpoena may not even be necessary depending on the provider's privacy policy. However, this is a question deserving of Fourth Amendment and privacy examination and therefore beyond the scope of our analysis. Assume, however, that no log files exist. It may still be reasonable to assume the use of cloud-based storage given the nature of the OS. The

[124] *See* Clemens, *supra* note 5, at 9; Reitinger, *supra* note 5, at 189-91; Ungberg, *supra* note 5, at 556-57.

[125] Clemens, *supra* note 5, at 9 (citations omitted).

[126] Ungberg, *supra* note 5, at 556-57.

[127] Peter Bright, *Surfing on the sly with IE8's new "InPrivate" Internet*, ARS TECHNICA (August 27, 2007, 9:10 AM), http://arstechnica.com/microsoft/news/2008/08/surfing-on-the-sly-ie8s-inprivate-internet.ars ("A cookie is a small, semi-persistent piece of data that is stored by your web browser and can be retrieved by the website that created the cookie in the first place.").

location of such storage, however, would be unclear. Consequently, we find ourselves in a situation analogous to *Doe*, and the government may end up compelling the accused to sign a release for any files that may hypothetically exist on a third-party's servers. The government could then approach all known storage providers, with the providers turning over the files should they exist. In practice, however, this presents several problems.

In *Doe*, the release form was drafted in such a manner as to avoid characterization as testimonial.[128] That is, by adding his signature to the form, the defendant did not communicate any information about the existence of any particular account.[129] Rather, the forms limited themselves to the hypothetical.[130] It fell upon the banks to confirm the existence of any such accounts. However, such a release may not be possible in the case of cloud computing given the manner in which such services are obtained. Consider, for example, the myriad of cloud-based services offered by Google.

In order to obtain a Google account and access to Google Docs, one of Google's cloud-based services, would-be users need only provide an email address to which they have access along with a password of their choice.[131] Should the would-be user not have an email address, it is a simple matter to first sign up for one through Google's Gmail service. Creation of a Gmail account requires only that the user provide her full name and that she select a login name and password.[132] Google's terms of service require that "any registration information [the user] give[s] to Google will always be accurate, correct and up to date."[133] There is, however, no attempt to confirm a user's name/identity. Consequently, in order to cooperate with a Government request to hand over data, Google may need more than the name and permission of the accused since an alias may have been used when creating the account. The simplest solution to this problem would be to provide Google with the account's login name or the alias used. Therefore, instead of a signature, the Government may try to compel the production of the login name or the alias, and here the problem is at least twofold.

In *U.S. v. Drew*, Lori Drew was indicted for felony violations of the Computer Fraud and Abuse Act for violating a website's terms of service agreement.[134] Subsequently, a jury found her guilty of several misdemeanor

[128] Doe v. United States, 487 U.S. 201, 203 (1988).

[129] *Id.* at 217-18.

[130] *Id.* at 203.

[131] *Create an Account*, GOOGLE ACCOUNTS, https://www.google.com/accounts/NewAccount (last visited March 5, 2010).

[132] *Id.*

[133] *Google Terms of Service*, GOOGLE TERMS OF SERVICE, https://www.google.com/accounts/TOS (last visited March 5, 2010).

[134] U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

violations.[135] She was later acquitted as the judge found the stated crime of unauthorized use of a computer void-for-vagueness.[136] However, given this is only one case in one jurisdiction, such a theory of criminal liability could find itself in court again. Under such a theory and given that the terms of service require users to provide accurate information, the use of an alias would in and of itself constitute a crime. Consequently, the production of that alias or the accompanying login name would serve to incriminate the accused in said crime, thereby triggering the Fifth Amendment's protection against self-incrimination. This is the first of the two problems presented by our most recent scenario. Law enforcement could no doubt grant the accused a closely tailored immunity to avoid implicating her right against self-incrimination,[137] agreeing not to prosecute for crimes deriving from the terms of service breach.

The second problem presented by our hypothetical, however, seems inescapable. The production of either the alias or the login name would likely qualify as testimonial under *Fisher*, as it would implicitly speak to the accused's control over an account whose existence was previously unconfirmed.[138] After all, the Government cannot compel the accused to communicate any factual assertion that "explicitly or implicitly" confirms the existence of documents, nor can the accused be compelled to "explicitly or implicitly" communicate his control over any such documents.[139] It would be as if in *Doe*, the government had asked Doe to sign a form naming the banks in which he had an account. Here the government may lean on reasoning similar to *Boucher II* and attempt to frame the existence of a cloud-based account as a foregone conclusion given the nature of the operating system. However, this seems analogous to compelling a murder suspect to produce the murder weapon. If he does, he clearly incriminates himself, having established his control over the weapon. Courts, however, have tried to argue that such a production would be acceptable as long as the government was able to link the weapon to the suspect after the fact through forensic evidence.[140] However, as was pointed out by the District Court in *Hubbell*:

> where the government had no evidentiary knowledge independent of that derived, directly and indirectly, from testimony communicated through compelled production, [the case law] clearly repudiate[s] any attempt to do so. [It] collectively teach[es] that the scope of the Fifth Amendment's protection cannot be measured by merely imagining that our [murder

[135] *Id.*

[136] *Id.*

[137] *See supra* notes 124-26 and accompanying text.

[138] Fisher v. United States, 425 U.S. 391, 408, 410-13 (1976).

[139] Doe v. United States, 487 U.S. 201, 210 (1988).

[140] United States v. Hubbell, 167 F.3d 552, 602 (C.A.D.C. 1999) (dissenting opinion).

> weapon] appeared, like manna from heaven, in the grand jury room.[141]

Given that the information stored in the cloud must first be communicated across a network, an alternative to forced production would be for the government to eavesdrop on the user for some time before making itself known, thereby gaining access to the information needed without requiring any cooperation on the part of the accused. All it needs to intercept is the relevant account information. After it has this, it will know what provider to approach and what account to ask for. It may also be possible to obtain some of this information after the fact by subpoenaing log files from the accused's internet service provider (ISP).[142] These files would likely not contain specific account information, but they may make it clear what sites the accused frequented and thereby narrow the list of possible cloud providers. However, it is important to note that there is no legal requirement for an ISP to hold on to such files for more than ninety days unless first asked by law enforcement[143] and many ISPs only maintain this data for a manner of months.[144] These records, if they existed, would likely match the user to an Internet Protocol (IP) address or clickstream which cloud providers could match with a particular account given sufficient context and logging on their part.[145] An IP address is a numerical label used by computers on the Internet to manage the delivery and receipt of information.[146] As its name suggests, it acts in much the same way as a physical address, allowing a user to access a service on the Internet which may then direct a reply to the user's IP address.[147] A website's URL is actually just an easy-to-remember pointer to the site's IP address.[148] A user's IP address is assigned by her ISP and is likely to change over time.[149]

Further complicating the government's attempt to discover the existence and control of information stored in the cloud is the availability of anonymizing networks such as that offered by the Tor Project. The Onion Router (Tor) makes use of a global computer network to obscure a user's IP address from

[141] *Id.* at 584-85 (citations omitted).

[142] *See e.g.*,, U.S. v. Bobb, 577 F.3d 1366 (11th Cir. 2009).

[143] 18 U.S.C. § 2703(f)(2) (2009).

[144] Ryan Singel, *Which ISPs Are Spying on You?*, Wired (May 30, 2007), http://www.wired.com/politics/onlinerights/news/2007/05/isp_privacy.

[145] *Id.* "[C]lickstream data includes every URL a customer visits, including URLs from search engines, which generally include the search term." *Id.*

[146] Alma Whitten, *Are IP Addresses Personal?*, Google Public Policy Blog (Feb. 22, 2008, 12:31 PM), http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html.

[147] *Id.*

[148] *Id.*

[149] *Id.*

the sites she visits by acting as an intermediary.[150] The ISP only sees the user connecting to the Tor network and the site the user is visiting only sees the IP address of the last computer in the Tor network, not that of the user.[151] Consequently, the ISP's records would not contain information specifying what sites the user visited after first accessing the anonymizing network, and the operators of the anonymizing network remain ignorant of such information by design.[152] Communications between users and networks such as Tor are often encrypted by public key encryption.[153] Therefore, even given real-time surveillance by the government, an account's location and existence would remain unknowable. However, if the government can guess what site the user was accessing, it could subpoena that site's records and attempt to match the user's activity with that of a user coming from the anonymizing network.[154] Systems such as Tor are good at preventing traffic analysis but not traffic confirmation; whereas traffic analysis attempts to discover what a user is doing from a single observation point, traffic confirmation attempts to confirm a hypothetical action on the part of the user given multiple observation points.[155] It is not clear, however, at what point a court would deem such a trial-and-error approach a fishing expedition.[156] Nor is it clear that all of the information necessary to connect a user to an account would be available absent real-time surveillance since ISPs need not retain data past ninety days.[157] The government could directly eavesdrop on the accused's activities, but retrospective discovery of existence and control seems increasingly uncertain with the passage of time. The government could ask cloud providers to cull their users' data, looking for file contents in an attempt to find any files that might belong to the accused, perhaps by keyword search or some other analytic means. This, however, would require cloud providers to search the contents of all of their users' files. Since the government does not even know where the files might reside or if they even exist, it would have to look through everyone's files everywhere. It is hard to see how this could stand up to the inevitable Fourth Amendment and privacy challenges, not to mention the practical challenges involved. The relevant Fourth Amendment analysis is beyond the scope of this paper. It is worth noting, however, that the

[150] *Overview*, TOR, http://www.torproject.org/overview.html.en#thesolution (last visited Nov. 27, 2010).

[151] *See id.*

[152] *See id.*

[153] *FAQ*, TOR, http://www.torproject.org/docs/faq.html.en (last visited Nov. 27, 2010).

[154] *See* arma, *One cell is enough to break Tor's anonymity*, THE TOR BLOG (Feb. 18, 2009), http://blog.torproject.org/blog/one-cell-enough.

[155] *Id.*

[156] *See supra* text accompanying notes 42-44.

[157] 18 U.S.C. § 2703 (f)(2) (2009).

government, in partnership with content hosts, has previously rationalized similar practices.[158]

C. A Coming Storm.

The Fifth Amendment issues presented to law enforcement above seem soluble given encryption's apparent susceptibility to *Fisher*'s foregone conclusion analysis and the fact that anonymizing networks likely constitute a small fraction of Internet users. Such a conclusion, however, may be premature. In the analysis of cloud computing above, we did not address the role of encryption as it related to the storage of data in the cloud. Nor did we entertain the possibility that an accused individual might make use of an anonymous ISP, such as a public wireless connection or wifi hotspot.[159] Taken together, these two additions, as a practical matter, appear to foreclose the possibility of establishing existence and control retrospectively.

In January 2010, Google announced that users of its Google Docs suite would be able to upload files of any type to cloud-based storage,[160] a functionality available from Microsoft's Windows Live SkyDrive since 2008.[161] This allows users to upload encrypted files, a functionality which has far-reaching implications for the reach of law enforcement's access to cloud-based storage.

Consider the following scenario similar to those laid out above. An individual has opened a Google Docs account based on an alias. She also has a copy of PGP on her computer. She has a number of documents she would like to store in the cloud. So she uses PGP to encrypt the files with traditional encryption. Afterwards she uploads the files to Google Docs and deletes the originals along with her browser history and any cookies stored on her computer. To do this, she makes use of a software program such as

[158] Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today (May 11, 2006, 10:38 AM), http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm; *Al Haramain v. Bush*, Electronic Frontier Foundation, http://eff.org/cases/al-haramain (last visited Nov. 27, 2010).

[159] Paul S. Henry and Hui Luo, *WiFi: What's Next?*, IEEE Comm. Mag., Dec. 2002, at 66, 66 ("WiFi, also known as 802.11b, has become the preferred technology for wireless local area networking in both business and home environments. . . . WiFi is also being deployed in public places to create so-called *hotspots*, where WiFi-capable users can obtain broadband Internet access.") (emphasis added).

[160] Vijay Bangaru, *Upload your files and access them anywhere with Google Docs*, Offical Google Blog (Jan. 12, 2019, 9:19 AM), http://googleblog.blogspot.com/2010/01/upload-your-files-and-access-them.html; *Uploading and exporting: Uploading any file*, Google Docs Help, http://docs.google.com/support/bin/answer.py?answer=50092 (last visited Nov. 27, 2010).

[161] Chloe Albanesius, *Google Docs Adds Cloud Storage For Any File*, PC Mag. (Jan. 12, 2010), http://www.pcmag.com/article2/0,2817,2357996,00.asp.

DeleteOnClick that securely deletes files, making them nearly impossible to recover.[162] Alternatively, she could be using a program such as Eraser, which wipes the free space on one's computer at predefined intervals, securely deleting the remnants of deleted files.[163] Such an approach used in combination with a browser feature such as "incognito," available in Google's Chrome browser, or Microsoft's "InPrivate" would leave no trace of the accused's activities.[164]

Now the government gains legal access to her computer and wants whatever files she may have stored in the cloud. The government has no knowledge of the Google account, but it suspects that there must be files somewhere. It seems clear that giving up any account information is testimonial as it would establish existence and control. It has been ninety days since she last accessed the files, and the ISP no longer has records covering her uploads. Of course, the government doesn't know this because it does not know that there were actually uploads. This lack of information means that even if the government

[162] DeleteOnClick is compliant with the U.S. DoD 5220.22-M secure file deletion standard. *DeleteOnClick*, 2BRIGHTSPARKS, http://www.2brightsparks.com/onclick/doc.html (last visited Nov. 27, 2010). Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine, *Threats to Privacy in the Forensic Analysis of Database Systems*, PROCEEDINGS OF THE 2007 ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGEMENT OF DATA, June 2007 ("Existing work in computer forensics has shown that in many operating systems and applications a deletion operation does not physically remove data. Researchers have studied the retention and recovery of expired data in file systems, random access memory, and such applications as web browsers and document files. . . . Military and intelligence agencies have set forth rigorous policies for the destruction of sensitive electronic data.") (footnotes omitted). *See National Security Industry Program Operating Manual (DoD 5220.22-M)*, DEFENSE SECURITY SERVICES, (Feb. 28, 2008), http://www.dss.mil/isp/odaa/documents/nispom2006-5220.pdf.

[163] Erica Sadun, *Download of the Day: Eraser*, LIFEHACKER (Sept. 13, 2005, 1:30 PM), http://lifehacker.com/software/downloads/download-of-the-day-eraser-125289.php.

[164] *Explore Google Chrome features: Incognito mode (private browsing)*, GOOGLE CHROME HELP, http://www.google.com/support/chrome/bin/answer.py?answer=95464&hl=en-US (last visited Nov. 27, 2010) ("For times when you want to browse in stealth mode, for example, to plan surprises like gifts or birthdays, Google Chrome offers the incognito browsing mode. Here's how the incognito mode works: []Webpages that you open and files downloaded while you are incognito aren't recorded in your browsing and download histories. []All new cookies are deleted after you close all incognito windows that you've opened."); *What is In Private Browsing?*, MICROSOFT.COM, http://windows.microsoft.com/en-US/windows7/What-is-InPrivate-Browsing (last visited Nov. 27, 2010). Additionally, a user may also want to disable Flash cookies to assure that there is no trace of their browsing history. Ryan Singel, *You Deleted Your Cookies? Think Again*, WIRED EPICENTER (Aug. 10, 2009, 7:39 PM), http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/.

could guess as to where the accused may or may not have uploaded files, it cannot make a connection based on a comparison with her ISP's log files because there are none. The only remaining retrospective method available is for them to search everyone's files everywhere. Ignoring the Fourth Amendment and privacy hurdles, even if the government could do this, it would fail to produce any results because the user's data is encrypted and so appears to be gobbledygook, and finding an encrypted file somewhere in the cloud tells us nothing about its origin. Confronted with such a challenge, the government may be tempted to build a backdoor into everyone's encryption technology so that it may read everything in the future, but such attempts have been met with great resistance in the past and probably would prove impractical.[165]

Now imagine the same scenario with a single alteration. Instead of using a traditional ISP, she makes use of a public wifi hotspot or "'Wi-Fi squatting,' using someone's unsecured wireless network without permission."[166] The availability of public wifi hotspots is growing rapidly.[167] McDonald's and Panera Bread offer free wifi and do not require users to identify themselves.[168] Additionally, unprotected personal wifi routers provide anonymous Internet access to anyone within range.[169] Unless the government can establish that the accused made use of one of these to access the Internet and unless that access point has kept detailed log files, the government is in exactly the same position as in the scenario above, except the upload could have occurred yesterday, not ninety plus days ago. It's important to note that neither of these two most recent scenarios required the user to make use of an anonymizing network. In fact, aside from the encryption and secure deletion, the user behavior above conforms to rather mainstream patterns of computer usage. Many Americans make use of wifi hotspots as well as Google Docs, and given a growing public understanding of computer security, it seems reasonable to assume that an increasing number of Americans or software developers will adopt secure deletion and file encryption as a matter of best practices. For example, the

[165] *See* A. Michael Froomkin, *Creating A Viral Federal Privacy Standard*, 48 B.C. L. REV. 55, 70-71 (2007); Bert-Jaap Koops and Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115, 146 (2005).

[166] Ben Worthen, *Best of the Business Tech Blog: Is Wi-Fi Squatting Wrong?*, WALL ST. J., Sept. 4, 2007, at B4.

[167] Matt Hamblen, *McDonald's free Wi-Fi part of growing trend*, COMPUTERWORLD (Dec. 17, 2009, 6:01 AM), http://www.computerworld.com/s/article/9142402/McDonald_s_free_Wi_Fi_part_of_growing_trend. *See e.g.*, Press Release, Panera Bread Operating Largest Free Hotspot Network in U. S. (Apr. 8, 2004), *available at* http://www.icoacorp.com/index.php?pid=224.

[168] Hamblen, *supra* note 167; Panera Bread Operating Largest Free Hotspot Network in U.S., *supra* note 167.

[169] *See* Worthen, *supra* note 166, at B4.

most recent release of Apple's operating system, Snow Leopard, included built-in secure deletion,[170] and although it is not implemented by default, it can be set as the default method.

Even if the above form of data encryption is not used, the encryption of data stored on the cloud is only relevant should the government seek to search the contents of all data in the cloud, and if we are to assume that they have yet to identify the files which they seek, it seems reasonable to expect that the Fifth Amendment's blocking of access to account information would be enough to put the brakes on the entire endeavor before getting to this point. This means that the end result is to place these files out of reach.

Consider what this means for a computer user who accesses cloud computing services only from wifi hotspots, who makes use of incognito mode, and who has scheduled Eraser to clean her hard drive daily or has reset her Apple settings to securely empty her "trash" by default. Unless the government knew for sure that she already had an account with some cloud provider, the act of production doctrine appears to present the functional equivalent of a complete bar to retrospectively accessing any files stored in the cloud. Of course, real-time surveillance may present a means for law enforcement to establish the data's existence and the accused's control. However, such an approach is far more intrusive and resource intensive than the retrospective discovery of evidence.

VI. WHAT RESULT?

It seems likely that Fifth Amendment issues surrounding encryption will soon find resolution. If that resolution involves a clear protection for the production of encryption keys under most circumstances, that protection will extend to cover encrypted data in the cloud. Such an outcome would make much of the above analysis unnecessary. Those wishing to imbue their data with Fifth Amendment protection would only have to encrypt their files. The history of Fifth Amendment jurisprudence, however, shows a flexibility that may result in a compromise solution,[171] and the consequences of such a compromise for cloud computing are unclear. It is conceivable that this compromise will later become subject to a further compromise brought about in response to the complications presented by cloud computing which in turn will be open to compromise when confronted with whatever technology follows. Consider this trajectory, including speculation about possible outcomes, as this may be helpful in formulating an optimal response.

[170] *Really Empty the Trash*, APPLE PRO-TIPS, http://www.apple.com/pro/tips/empty_trash.html (last visited Nov. 27, 2010).

[171] *See* Stuntz, *supra* note 60; Hon. Alan G. Gless, *Self-incrimination Privilege development in the Nineteenth-Century Federal Courts*, 45 AM. J. LEGAL HIST. 391 (2001).

A. *Holding the Line*

Under the current act of production doctrine and given current technology, it appears that casual Internet users making use of wifi hotspots and cloud computing are only a small step away from imbuing their data with protection under the Fifth Amendment's privilege against self-incrimination, assuming of course that their data contains some incriminating content. A lack of log files on their computer is all that is needed for this approaching storm to manifest, and although this is unlikely to occur by chance, the tools necessary to bring it about are easily accessible. Chrome's incognito mode is just a click away,[172] and Eraser can be set up to do its work in the background.[173] What are we to do in the face of this approaching storm? Privacy advocates might suggest that we do nothing, and this is a defensible position. The founders were aware of the tension between privacy and transparency, and yet they chose to enshrine a protection against self-incrimination as part of the Fifth Amendment. However, our technology has become a force multiplier. At our nation's founding, it was inconceivable that nineteen people could kill nearly three thousand while destroying millions of dollars in property by hijacking three commercial transports. Consequently, it is easy to understand why many in law enforcement seek easier access to data, be it through legal or technical channels. It is not clear, however, what balance is proper. The December 2009 cyber attacks on Google targeting the Gmail accounts of human rights activists[174] along with the use of cloud-based social media sites by protesters in the wake of Iran's disputed 2009 elections[175] make clear the importance of personal security and anonymity in the cloud. Such events will no doubt lead companies like Google to provide greater security within the cloud, perhaps even restricting their own ability to access user content, thereby arriving at the same results as the hypothetical cloud-based encrypted files above. If nothing is done, retrospective discovery of an accused's actions in the cloud may often become a legal and technical impossibility.

B. *Shifting Tactics*

Of course, even if the government does not implement new regulations or adopt new legal interpretations, law enforcement will adapt to the constraints

[172] Speakingtree, *How to Turn on Incognito Window in Chrome*, EHOW, http://www.ehow.com/how_4527279_turn-incognito-window-chrome.html (last visited Nov. 27, 2010).

[173] Sadun, *supra* note 163.

[174] David Drummond, *A New Approach to China*, OFFICIAL GOOGLE BLOG (Jan. 12, 2010, 3:00 PM), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[175] Evgeny Morozov, *Iran Elections: A Twitter Revolution?*, WASH. POST (June 17, 2009, 3:00 PM), http://www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html.

placed upon it. The examples above point to the direction in which that adaptation is likely to lead. It seems that the only viable option for law enforcement is the adoption of more intrusive surveillance, be it after-the-fact queries of the entire cloud or real-time surveillance. A similar pressure is exerted by encryption technology and has led to the "hovering" of government agents.[176] In *United States v. Scarfo*, after an original search uncovering encrypted files, the government was forced to pursue a second warrant authorizing the placement of key-tracking software on Scarfo's computer in an attempt to discover his PGP password.[177] This required an extended period of surveillance, which opened Scarfo up to far greater scrutiny than would have occurred had such measures been unnecessary.[178]

It seems reasonable to speculate that in the face of continued pressure from unbreakable codes and unknowable hiding places, law enforcement will necessarily push the boundaries of surveillance.[179] The court in *Scarfo* noted that:

> [w]here proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence. . . . "[T]he complexity of an illegal scheme may not be used as a shield to avoid detection when the [government] has demonstrated probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession."[180]

This tightened scrutiny raises the question as to whether the solution may be worse than the ill it aims to avoid.[181] It is easy to see how a similar argument could be made in relation to issues arising from the cloud.

C. Regulation & New Technology

A look at the history of encryption is illustrative. In the 1990s, there was growing fear from the U.S. government that its ability to listen in on criminals

[176] *See* Ungberg, *supra* note 5, at 549-51 (citing *generally* Rachel S. Martin, Note, *Watch What You Type: As the FBI Records Your Keystokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 AM. CRIM. L. REV. 1271 (2003) (discussing warrants designed primarily to uncover computer passwords)).

[177] United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

[178] *Id.*

[179] *See, e.g.*, Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 4 (2008); Ungberg, *supra* note 5, at 549-51.

[180] *Scarfo*, 180 F. Supp. 2d at 578 (D.N.J. 2001) (quoting Andresen v. Maryland, 427 U.S. 463, 482 n.10 (1976)).

[181] Ungberg, *supra* note 5, at 551.

would soon be compromised by the development of strong encryption.[182] In an attempt to address this concern, they introduced the idea of the Clipper Chip.[183] The Clipper Chip was an umbrella name given to a collection of encryption technology that would be made available to the public.[184] No one would be required to use this technology, but those who did would receive strong encryption and the ability to keep secrets from most of the world in exchange for allowing a government backdoor to their data.[185] Much to the government's dismay, this solution was poorly received, and those retailers that included the Clipper technology failed to sell many products. The public voted with their pocketbooks, and they rejected the government's attempt to listen in.[186] However, in November 2010, the Obama administration signaled that it would introduce legislation similar in spirit to the Clipper chip, requiring communications providers to allow access to encrypted content.[187]

An analogous solution could be presented for cloud computing, perhaps guidelines for the registration of verified identities with cloud providers. However, such a solution is likely to encounter resistance, especially from those companies like Google that have exploited the low bar of participation that comes with anonymous free usage. In the absence of such a requirement, it is hard to imagine what incentive could be used to induce end users to undergo such verification. It is possible that distributed trust networks[188] may bring about some type of centralized authentication which providers could implement, but unless mandatory, such a scheme lacks teeth. It should be noted, however, that there are many justifiable and even laudable rationales behind Internet anonymity.[189] Additionally, given the global nature of cloud-based services, it seems unlikely that a single global legal requirement could be reached.[190] A less intrusive solution might be the implementation of data

[182] Froomkin, *supra* note 165, at 70.

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.* at 71.

[187] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1.

[188] Aifarez Abdui-Rahman & Stephen Hailes, *A Distributed Trust Model*, PROCEEDINGS OF THE 1997 WORKSHOP ON NEW SECURITY PARADIGMS 48 (1997).

[189] *See Scarfo*, 180 F. Supp. 2d at 574; *Who Uses Tor?*, TOR: ANONYMITY ONLINE, http://www.torproject.org/torusers.html.en (last visited March 5, 2010). *See also* karsten, *Measuring Tor and Iran (Part two)*, THE TOR BLOG, (July 1, 2009), http://blog.torproject.org/blog/measuring-tor-and-iran-part-two.

[190] Some commentators have suggested that law enforcement's job will be made easier by new Internet technological standards such as Internet Protocol version 6 (IPv6), the next-generation of technical rules set to govern the Internet. Along with other innovations, IPv6 may make it easier to connect individual users with their online behavior. *Compare* Bill

retention laws requiring ISPs to maintain records for some reasonable amount of time, which could then be matched with users after the fact. Such an approach is being pursued by law enforcement.[191] As the previous scenarios illustrate, even this is insufficient to address all circumstances under which problems will arise. Data retention by ISPs makes little difference should the accused make use of an anonymous ISP such as the wifi at the local coffee shop.[192]

D. Narrowing the Law

The history surrounding the act of production doctrine demonstrates a flexibility that may be responsive to the needs of law enforcement.[193] In fact, the doctrine has shown such flexibility that some commentators look back to *Boyd* and see wholesale dismantling of the Fifth Amendment's protection against self-incrimination.[194] In other countries, the failure of technical measures to grant law enforcement with access to encrypted data has resulted in legal fixes, namely, laws which compel the production of encryption keys.[195] The Netherlands enacted such a law in 1993, followed by the UK,

Frezza, *Where's all the outrage about the IPv6 privacy threat?*, 783 INTERNETWEEK 43, (October 4, 1999), available at http://www.ipv6.ru/russian/presscenter/press/ebsco/1.php); Steve Deering & Bob Hinden, STATEMENT ON IPV6 ADDRESS PRIVACY (November 6, 1999), http://playground.sun.com/ipv6/specs/ipv6-address-privacy.html.

[191] Declan McCullagh, *FBI, politicos renew push for ISP data retention laws*, CNET NEWS (April 23, 2008, 10:50 AM), http://news.cnet.com/8301-13578_3-9926803-38.html.

[192] Even if we took the draconian step of extending data retention laws to include a log of every coffee shop patron, users in neighboring locations might access the shop's wifi network. We could require identity verification to access the network, but this would run counter to the business model of many wifi providers who rely on free wifi access to get patrons in the door. Again, a solution to tracking user behavior may be more surveillance. *See* Erik Larkin, *Browser Fingerprints: A Big Privacy Threat*, PC WORLD (March 26, 2010, 9:00 PM), http://www.pcworld.com/article/192648/browser_fingerprints_a_big_privacy_threat.html.

[193] *Gless*, *supra* note 171.

[194] *Id*. at 391 ("No person charged with a crime may be compelled to testify in person as a witness for the government at the person's own criminal trial. However, any person may be compelled to be a witness against himself or herself, in any criminal case, including in his or her own criminal trial, through the use of various forms of compulsion, which the current Court majority considers acceptable, including, but not limited to: immunized testimony, custodial and non-custodial interrogation, the forced submission of breath samples, bodily fluids, fingerprints, photographs, papers classifiable as required records, and even most papers recognized to be private in almost any other context, with refusal to cooperate constituting admissible evidence of guilt, along with any statements made under any of the acceptable forms of compulsion, any volunteered statements, and other statements made voluntarily.").

[195] Bert-Jaap Koops and Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12

Belgium, and France.[196]

In the preceding sections, it is observed that a failure to compromise in the application of the doctrine may result in increasingly Orwellian measures on the part of law enforcement as it attempts to navigate a path around the technical barriers presented by ever changing technology. It is worth noting that the precedents established today are likely to remain in place for the foreseeable future. Take for example the development of functional magnetic resonance imaging (fMRI) as a tool to infer the contents of one's mind. In 2008, scientists at the Computational Neuroscience Laboratories in Kyoto, Japan were able to construct images of what someone was looking at from brain scans,[197] and in 2010, researchers at University College London announced that they had been able to accurately determine what subjects were remembering based upon similar scans.[198] Although it likely remains in the distant future, this technology is the precursor to technology capable of recording our dreams, our memories, and perhaps our waking thoughts.[199] A number of companies already exist dedicated to using fMRI as a lie detector.[200] How will the Fifth Amendment deal with such technology once it has grown beyond its infancy? If the scanning of one's brain is a passive activity, does it implicate compulsion, or is it like the production of blood? What about the day when it becomes routine to archive memories in the cloud? When deciding how to address the concerns presented by cloud computing, it is worth asking, "where will this all lead?" As people come to store the majority of their data in the cloud, how do we protect it, and what balance do we strike with the state's interest in accessing it?

VII. CONCLUSION

No matter what the testimonial nature of an encryption key, the location of cloud-based data is likely to be protected by the act of production doctrine as long as the government lacks specific knowledge as to the existence and control of any potential files. The much hyped iPad and netbooks running Google Chrome OS are being billed as cloud-based devices, and Microsoft CEO, Steve Ballmer, has recently said that "about 70 percent of [Microsoft's

MICH. TELECOMM. & TECH. L. REV. 115, 148-49 (2005).

[196] *Id.*

[197] Celeste Biever, *'Mind-reading' software could record your dreams*, THE NEW SCIENTIST (Dec. 12, 2008, 7:05 PM), http://www.newscientist.com/article/dn16267-mindreading-software-could-record-your-dreams.html.

[198] Kyle VanHemert, *Brain Scans Can Access Your Memories*, GIZMODO (Mar. 16, 2010, 1:00 AM), http://gizmodo.com/5494174/brain-scans-can-access-your-memories.

[199] Biever, *supra* note 197.

[200] Steve Silberman, *Don't Even Think About Lying*, WIRED (Jan. 2006), http://www.wired.com/wired/archive/14.01/lying.html.

engineers] are [currently] doing things that are entirely cloud-based, or cloud-inspired. And by a year from now that will be 90 percent."[201]

Given current and near-future cloud computing solutions and current patterns of cloud usage, ignorance on the part of the government is to be expected for two subsets of the population: those actively hiding their tracks and those who have slipped through the cracks. On one hand, the recent Google cyber attacks illustrate the vulnerability of information stored in the cloud, a fact that will likely drive increased user security, perhaps prompting Google to actually promote features such as incognito which are important steps in hiding user data from prying eyes. On the other side, the ability of small groups of individuals to effect carnage through the use of online information sharing, such as in the 2008 Mumbai attacks,[202] argues in the opposite direction.

It seems clear that in the future we will place more and more of ourselves in the cloud, meaning that the decisions made today about the cloud may one day apply to nearly all of our "papers." Technology may make online surveillance easier over time, or it may make it more difficult, but the entirety of the problems facing a fully connected world deserve thoughtful consideration from our courts and legislatures. It seems possible that a shortsighted application of law to the cases at hand may improperly weigh near-term gains against distant losses. Centuries from now, when copies of our memories are routinely archived on the cloud, will they be protected by the privilege of production? Will the Fifth Amendment right against self-incrimination become functionally obsolete? All that is certain is this: a storm is coming.

[201] Steve Ballmer, *Cloud Computing*, MICROSOFT NEWS CENTER (Mar. 4, 2010), http://www.microsoft.com/presspass/exec/steve/2010/03-04Cloud.mspx.

[202] Rahul Bedi, *Mumbai attacks: Indian suit against Google Earth over image use by terrorists*, THE DAILY TELEGRAPH (Dec. 9, 2008, 6:25 PM), http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html.