Washington Journal of Law, Technology & Arts

Volume 5 | Issue 3 Article 3

1-1-2009

The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model

Kristina Ringland

Corporate & Commercial
Cite as: Kristina Ringland, *The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model*, 5 SHIDLER J. L. COM. & TECH. 13 (2009), *available at* <http://www.lctjournal.washington.edu/vol5/a13Ringland.html>

THE EUROPEAN UNION'S DATA RETENTION DIRECTIVE AND THE UNITED STATES'S DATA PRESERVATION LAWS: FINDING THE BETTER MODEL

Kristina Ringland[1]

Abstract

The European Union's Data Retention Directive (the "Directive") seeks to assist law enforcement officials in their efforts to combat terrorism and to standardize disparate laws regarding data retention within the European Union (EU). The Directive requires companies to retain traffic and location data that identifies a subscriber or registered user of a Web site for a period of six to twenty-four months. Implementation of the Directive takes place at the national level and poses many challenges to providers of electronic communication services. There is no analogous United States federal law mandating data retention. The United States, however, has a data preservation requirement, which pertains only to specific information requested by the United States government. This Article compares the two distinct approaches and examines which approach better balances the interests of law enforcement officials combating terrorism, and the cost to companies and consumers to comply with the laws. This Article concludes that the United States's current legal framework of data preservation strikes a more favorable balance between these competing interests.

Table of Contents

INTRODUCTION

Data storage presents a complex and costly challenge for many companies. Recent terrorist attacks in Europe and the United States (U.S.), notably the 2004 Madrid commuter train bombings and September 11 attacks, increased lawmakers' focus on the issue of data storage due to the public's strong desire to provide law enforcement with the power to access necessary electronic information.[2] The EU and the U.S. took different approaches to these new concerns: the U.S. adopted the USA Patriot Act,[3] which made minor changes to the existing data preservation model. The EU, by contrast, passed the Data Retention Directive.[4]

In implementing data storage laws, there are many competing factors to consider, including aiding law enforcement, the overall costs, and the intrusion into an individual's private information.[5] This Article examines the EU's Directive and the U.S.'s data preservation laws, and considers which model better balances these competing factors. In particular, the Article focuses on the United Kingdom as a case study to explore specific problems regarding the Directive's ambiguous terms and the costs of data retention.[6] This Article concludes that the U.S.'s data preservation laws provide a better framework for assisting law enforcement, while minimizing corporate costs and protecting public privacy. Finally, the Article briefly considers the likelihood that the U.S. will adopt a legal framework for data retention similar to the EU's Directive, given proposed data retention legislation.

THE EUROPEAN UNION'S DATA RETENTION DIRECTIVE

The EU's adoption of the Directive represents a shift away from prioritizing data privacy rights that the EU has historically protected.[7] Prior to the Directive, electronic communications services and public communications networks were only allowed to store a customer's traffic and location data as long as was necessary.[8] In addition, such services and networks were also required to either erase or make the data anonymous when the data was no longer needed for billing purposes.[9] Given the EU's framework of protecting users' privacy rights, the Directive effects providers of electronic communication services by requiring such providers to retain large amounts of traffic and location data, instead of retaining only data necessary for billing purposes; this shift in priority results in an increase in costs to retain and secure the data.[10] Thus, the main criticisms of the Directive focus on two issues: (1) the overall costs of retaining data and (2) the privacy of end users.[11] However, the overall costs to providers of electronic communication services and consumers would vary depending on how the member states transpose the Directive.

The Legal Framework of the Directive

The EU's Directive imposes several new restraints on providers of electronic communications services. For example, the Directive requires providers of electronic communication services to retain traffic and location data, which identifies the subscriber or registered user for a period of six to twenty-four months.[12] The Directive mandates that fixed network and mobile telephony providers, as well as Internet access, email, and Internet telephony providers,[13] must retain data regarding traffic and location of users; however, providers are not required to retain the content of the transferred data.[14] In addition, data to be retained does not include web pages visited.[15]

Significantly, EU member states must transpose the Directive into national law for the Directive to become effective. The Directive was passed on March 15, 2006[16] and had an implementation deadline of September 15, 2007 for telecommunications companies.[17] Internet data, by contrast, had an extended deadline of March 15, 2009.[18] While the implementation deadlines have already passed, many countries, including the United Kingdom, opted to postpone implementing legislation requiring Internet service providers to comply with the Directive until the extended deadline.[19] Accordingly, some of the impacts of the Directive have yet to be seen.

Technical Requirements for Providers of Electronic Communication Services

Complying with the Directive poses a technological challenge for providers of electronic communications services. Providers must, at a minimum, store the data, ensure its security, and access the data within a reasonable time period. Thus, major issues for electronic service communications providers remain: (1) the management of the data; (2) the ability to access data quickly;[20] and (3) balancing these issues with customer privacy expectations. To manage and preserve the data, logs should be stored centrally and include time stamps, digital signature, encryption and other precautions to prevent tampering.[21] However, the overall volume of data that service providers must manage to comply with the Directive is estimated to be in the tens or hundreds of terabytes for larger operators.[22] To comply with the Directive's requirement that the data be available within a reasonable time period, the systems must have both sufficient processing power and storage capabilities; indeed, this can be both costly and technically difficult for a wide range of companies.[23]

The Language of the Directive is Unclear

In addition to the technical challenges of implementing the Directive, ambiguities in the Directive's language pose problems for companies operating throughout the EU. The overall lack of clarity is particularly problematic for Internet service providers, telecommunications companies and individuals whose data is being retained.[24] For example, Article 8 explains that the data must be retained in such a way that it can be transmitted to the competent authority without undue delay.[25] However, the language of Article 8 presents problems because of the possible interpretations of both the terms "competent authorities" and "without undue delay." If a country interprets "competent authorities" broadly, companies will be required to retrieve substantially more data and will have significantly greater expenses. The United Kingdom, for instance, did not clarify competent authorities when it implemented the Directive with regard to telecommunications data.[26] As such, companies are left to interpret if the United Kingdom's regulation has a broad scope. Germany and Holland, on the other hand, limited competent authorities to crime and law enforcement agencies.[27]

The phrase "without undue delay" also presents numerous problems for companies attempting to plan for the implementation of the Directive. "Without undue delay" could refer to hours, days, weeks or months.[28] Given the large amounts of data that companies must retain, organizing the data in a manner that allows this data to be searched and transmitted quickly results in a high cost.[29] Again, the United Kingdom's regulation fails to clarify the time frame expected, but retains the language of "without undue delay."[30]

Cost Considerations for the Directive

Although determining the Directive's cost to companies is difficult, estimates reveal the cost is considerable. A major issue that arises from the Directive's implementation is whether companies or the member states' governments will bear the cost of these new requirements via reimbursement.[31] The Directive is silent as to which party will pay for the storage and access of the data. Such decisions are instead left for national governments to resolve when transposing the Directive into national law. When attempting to comply with a national act similar to that of the Directive—the United Kingdom's Anti-Terrorism, Crime, and Security Act—America Online (AOL) estimated that it would cost thirty million pounds to set up a data retention system, and another thirty million pounds to run the system each year.[32] Another Internet expert estimated that the cost for its company would be around five to six million pounds.[33] Such estimates demonstrate that companies implementing the Directive will incur substantial costs.

However, countries vary as to whether the national government will reimburse private corporations for expenses associated with complying with the Directive.[34] Under the United Kingdom's previous voluntary data retention law,[35] the government contributed a reasonable proportion of the marginal cost to a corporation if the retained data was for national security instead of retail purposes, and if the retention period was significantly longer than the business timeframe.[36] The current United Kingdom's regulations state: "The Secretary of State may reimburse any expenses incurred by a public communications provider in complying with these Regulations."[37] The regulations clarify that reimbursement may be conditional on whether the Secretary of State has been notified and has agreed to the expenses in advance.[38] The vague language of "may reimburse," coupled with the requirement that the expenses be agreed upon by the Secretary of State in advance, creates a problem for companies attempting to plan for the costs associated with the Directive.

Unlike the United Kingdom, Italy did not provide companies compensation for their data retention expenses under its previous data retention laws.[39] Given its background, it seems highly unlikely that Italy will reimburse companies for complying with the Directive. Denmark—the first country to implement the Directive for both telecommunications and Internet data—has a law that is silent on the issue of compensation,[40] signifying that companies will most likely be footing the bill. Therefore, while the Directive's cost appears considerable, the direct cost to companies depends on the implementation at the national level.

DATA PRESERVATION IN THE UNITED STATES

In the U.S., the current laws require data preservation and not data retention. Unlike data retention, which requires companies to retain all traffic information for a certain time period, data preservation only pertains to specific information requested by the government. Data preservation, as defined by the U.S. Internet Service Provider Association, is "the preferred mechanism to minimize the risk of deletion of records and communications that may be necessary during an investigation of a crime."[41]

The Legal Framework of Data Preservation

Under U.S. law, which also assists law enforcement in gathering electronic information, the framework for data preservation is known as the Electronic Communications Privacy Act of 1986 ("ECPA").[42] The ECPA requires different legal processes depending upon the type of electronic information requested by law enforcement.[43] Under the ECPA, three methods are available for obtaining electronic information: (1) a search warrant; (2) a

court order pursuant to 18 U.S.C. § 2703(d);[44] and (3) a subpoena.[45] Each method corresponds with a different level of privacy protection afforded to the type of record.[46] For example, to obtain content information, a court-ordered search warrant is necessary.[47] However, law enforcement may request traffic data be preserved and subsequently receive access to this data once a subpoena or a court order is granted.[48]

The Functionality of Data Preservation

The section of the ECPA that sets forth data preservation is 18 U.S.C. § 2703. The statute requires a provider of electronic communication services or remote computing services to retain records for ninety days, following a government entity's request for particular records to be retained.[49] Under the ECPA, companies do not retain information unless the government specifically requests that certain data be retained.[50] Once the government requests that the company preserve the data, the government must then proceed through the proper legal channels to gain access to the preserved records within ninety days and provide the Internet service provider with the legal basis for obtaining the data.[51] Given the current law, as a practical matter, most Internet service providers in the U.S. preserve data for thirty to ninety days as a minimum standard.[52] Internet service providers often discard data that is no longer necessary for business purposes, such as network monitoring, fraud prevention or billing disputes;[53] however, U.S. law does not require Internet service providers to destroy this data within a certain time period.

The Patriot Act amended parts of the ECPA, increasing law enforcement access to electronic information and decreasing consumer data privacy. The Patriot Act allowed Internet service providers to voluntarily disclose traffic and location data to law enforcement in limited circumstances.[54] The Patriot Act also expanded the information available to law enforcement via subpoena.[55] Through these amendments, a subpoena is all that is necessary to obtain a customer's Internet protocol address assigned to the consumer by the service provider. Furthermore, only a subpoena is required to obtain the source and mode that a customer uses to pay his or her communications provider, including a credit card or bank account number.[56] Given the elaborate nature of the U.S. data preservation system, costs again prove to be a difficult issue for most electronic service providers and other similarly situated corporations.

Cost Considerations for the United States's Data Preservation

Unlike the European Directive, the U.S. statutory framework explicitly declares which party should bear the costs. 18 U.S.C. § 2706 requires the government entity obtaining records or other information from a private service provider to reimburse the costs that are reasonably necessary for the provider making available the information.[57] Section 2706 further provides that the amount of the fee is either mutually agreed upon by the government entity and the providing party, or is decided by a court.[58] Since the cost of data preservation includes not only the expense of assembling the information, the statute also provides for payment due to the corporation for disrupting the normal operations of the providing entity.[59] Government entities, aware that preservation requests may be burdensome, occasionally negotiate the scope of the request to reduce the burden on the party receiving the request.[60]

DATA PRESERVATION: A BETTER MODEL?

Many EU member states have postponed transposing the Directive into national law with respect to Internet companies, which indicates a potential weakness in the data retention model. As demonstrated in the United Kingdom, a possible reason for delaying the implementation of the Directive is opposition from Internet companies because of anticipated costs.[61]

Prior to the Directive being passed, an Internet service industry statement explained that communications service providers preferred data preservation to data retention because "mandatory retention . . . is neither economically efficient nor effective for criminal investigation."[62] This statement asserts that data preservation specifically targets information that law enforcement needs to aid in investigations instead of merely keeping all data regardless of the purpose.[63] Furthermore, when the United Kingdom invited the public to comment on draft regulation aimed at transposing the Directive,[64] many respondents felt the complex issues surrounding the Internet resulted in the regulations being inappropriate and difficult to implement.[65] The Internet Service Provider Association—a group that represents 95% of the United Kingdom Internet access market by volume—believed the draft regulations "would not enable implementation of the Internet aspects of the Directive."[66] Respondents continued to be concerned with the cost for data storage and the potential retrieval of Internet communications.[67] Thus, the private sector appears to prefer the data preservation framework.

However, in spite of the already prevalent problems with implementing the Directive that may indicate flaws in the legal model, it remains difficult to determine whether the Directive or the U.S. data preservation laws provide a better legal framework. For example, from the law enforcement standpoint, investigations often occur six months to a year after an incident, and important information would likely be lost without certain data *retention* requirements. In addition, the cost of implementing a data retention law in the U.S. would likely vary from the projected costs in Europe, due to the fact that some U.S. companies already voluntarily retain their records.[68] As such, the cost of data retention in the U.S. would include only the cost for companies to either increase the length of their current data retention strategies, or the overall cost to retain the data for companies that currently do not voluntarily keep such data. The problem in accurately predicting these costs is that industry provides the data itself and may present only the data that reflect its interests, as noted above in reference to the United Kingdom's implementation of the Directive.[69]

All things considered, the data preservation model appears to strike a better balance by providing support to law enforcement and minimizing costs to service providers and their consumers. The Directive, however, does enhance law enforcements' ability to gain access to traffic and location data because all of the relevant information would be retained instead of deleted.[70] Nevertheless, access to dated material can be costly and of limited utility to law enforcement.

The U.S.'s data preservation laws, by contrast, minimize private and public costs by targeting particular users and setting specific timelines. Moreover, under 18 U.S.C. § 2706, a government entity must reimburse the company from which it is seeking the electronic information. Regardless, given the Patriot Act's amendments allowing Internet service providers to voluntarily disclose traffic and location data in certain circumstances,[71] neither the Directive nor the current U.S. preservation laws provide Internet users a high level of data privacy.

THE FUTURE OF DATA RETENTION IN THE UNITED STATES

In recent years, legislation has been proposed in the U.S. that would require companies to hold on to data for specific time periods without the requirement of a government request.[72] Such proposed legislation would result in the U.S. having a law that mirrors the EU's Directive. While there have been political overtures in the U.S., the likelihood of a data retention law actually coming into effect in the U.S. remains to be seen.[73] Proposed legislation would apply to Internet service providers and require retention for a period to be determined by the Attorney General.[74] In addition, proposed legislation does not state that the federal government will assist companies in complying with requirements to retain data. The vagueness in the statutory language would prove troublesome for compliance by Internet service providers, similar to the issues that are problematic under the Directive. Furthermore, such legislation may encounter fierce opposition from Internet service providers and the public on a number of grounds.[75]

CONCLUSION

The terrorist attacks in both Europe and the U.S. generated a desire to increase law enforcement's access to information. The EU passed the Directive to aid law enforcement in obtaining traffic and location data from telecommunications companies and providers of electronic communications services. The European situation displays the difficulties companies face when data retention laws are implemented, with regard to both clear legislative language and the cost of retaining the data. The current law in the U.S., however, is data preservation. Data preservation achieves a better balance between assisting law enforcement in criminal investigations while minimizing the costs to both corporations and consumers. Neither model effectively balances the privacy interests of consumers. Depending on the outcome of the Directive and the political movements in the U.S., the U.S. may move toward data retention in the future. Internet companies in the EU and the U.S. must be aware of data retention laws because these laws greatly impact both planning and costs.

PRACTICE POINTERS

- Although the March 2009 deadline has passed, companies connected to Internet access, Internet telephony, and Internet email that operate in Europe, should be aware of the various nuances regarding the implementation of the Directive within each EU member state.
- Companies should monitor pending U.S. data retention legislation, particularly regarding the overall vagueness of proposed laws and any language identifying which party would be required to cover the data retention costs.

<< Top

Footnotes

1. Kristina Ringland, University of Washington School of Law, J.D. program Class of 2009. Thank you to Professor Jane K. Winn of the University of Washington School of Law and Associate Vice Provost Bill Yock of the University of Washington, Thomas Daemen of Microsoft Corporation, Ivan Orton of the King County Prosecutor's Office in Seattle, Washington, and Karen Horowitz for their help with this Article.

2. Thomas Daemen, *The New European Union Data Retention Directive: Overview and Compliance Challenges*, SciTech Law., Summer 2007, at 14.

3. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USA Patriot Act].

4. Council Directive 2006/24/EC, 2006 O.J. (L 105) 54 [hereinafter Directive], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML.

5. This Article primarily focuses on implementation challenges and not the privacy concerns. *See generally* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233 (2007) (discussing privacy concerns and the Directive).

6. For the purposes of this Article, the United Kingdom is used as a case study since its experiences are representative of those of most European Union countries. Translations of many countries' laws are unavailable and, therefore, an exhaustive examination of each member nations' implementation of the Directive was not possible.

7. Bignami, *supra* note 5, at 238.

8. The Directive applies to data generated or processed by "publicly available electronic communications services" or "public communications networks." Both electronic communications services ("ECSs") and public communication networks ("PCNs") are well-established terms in European law. *See* Directive 2002/58/EC, 2002 O.J. (L 201) 37. The term "electronic communication services," as it is used throughout this Article, is meant to encompass both ECSs and PCNs.

9. Stuart Goldberg, *Legislative Comment: Data Retention Regulations 2007 Come Into Force*, Comm. L. 12(5), 165-66 (2007) (U.K.) (discussing Directive 2002/58/EC, 2002 O.J. (L 201) 37). The privacy directive was a European Union level mandate and member states had their own data retention rules that arguably conflicted with the European Union privacy requirements.

10. *Id.*

11. Mònica Vilasau, *Traffic Data Retention v Data Protection: The New European Framework*, Computer & Telecomm. L. Rev. 13(2), 53 (2007) (U.K.).

12. Directive, *supra* note 4, at art. 6.

13. Telephony is defined as follows: "the use or operation of an apparatus (as a telephone) for transmission of sounds as electrical signals between widely removed points." Merriam-Webster OnLine, http://www.webster.com/dictionary/telephony (last visited Apr. 26, 2008).

14. *See* Daemen, *supra* note 2, at 16 (elaborating the types of data that must be retained).

15. Jeff Goodall, *Data Retention: Transposition of the Data Retention Directive into Law*, Data Protection L. & Pol'y, Apr. 2007, *available at* http://www.kemplittle.com/html/stay-posted/publications/short-lines/data-retention-jig-may07.html?PHPSESSID=27b4283ef6769112f20a46eadddea41f.

16. Bignami, *supra* note 5, at 238.

17. Directive, *supra* note 4, at art. 15.

18. *Id*. It is important to note that while this deadline has already passed, directives are often implemented after the deadline.

19. 16 of 27 member states have delayed implementation on the issue of Internet data. For declarations from various countries that explain their decisions to postpone retention of communications data relating to Internet access, Internet telephony, and Internet email, see generally Directive, 2006/24/EC, 2006 O.J. (L 105) 54, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

20. Dave Bailey, *How Data Rules Will Burden Business*, IT Wk., Oct. 6, 2006, http://www.itweek.co.uk/itweek/analysis/2165870/rules-burden-business.

21. Ross Brewer, *Data Retention – Time and Tide Wait for No Man*, European Comm., Jan. 3, 2008, http://www.eurocomms.com/features/112061/_DATA_RETENTION_-_Time_and_tide_wait_for_no_man.html.

22. Fernando Elizalde, Senior Industry Analyst, Frost & Sullivan, *EU Data Retention Directive: An Onerous Burden on Service Providers* (Sept. 30, 2006), http://www.frost.com/prod/servlet/market-insight-top.pag?docid=83098430; *see also* Bailey, *supra* note 20 (describing the amount of data telecom companies need store in order to comply with the directive).

23. Industry has already responded to these challenges with new products that ISPs can purchase to implement the Directive. *See* OSS News Reviews, EM and Intec and SenSage Technology to Identify Terrorist Activity in Call Detail Records, http://www.ossnewsreview.com/telecom-oss/emc-and-intec-and-sensage-technology-to-identify-terroritst-activity-in-call-detail-records/ (last visited Sept. 21, 2009).

24. Gareth Davies & Gayle Trigg, *Being Data Retentive: A Knee Jerk Reaction*, Comm. L. 11(1), 18-21 (2006) (U.K.).

25. Directive, *supra* note 4, at art. 8.

26. *See* Data Retention (EC Directive) Regulations, 2007, S.I. 2199 (U.K.); *see also* Goodall, *supra* note 15.

27. Goldberg, *supra* note 9.

28. Goodall, *supra* note 15.

29. Daemen, *supra* note 2, at 15.

30. Data Retention (EC Directive) Regulations, 2007, S.I. 2199, art. 7 (U.K.); Goodall, *supra* note 15.

31. *See* Goodall, *supra* note 15.

32. Matt Loney, *ISPs Spell Out True Cost of Data Retention*, ZDNet.co.uk, Dec. 12, 2002, http://news.zdnet.co.uk/itmanagement/0,1000000308,2127408,00.htm.

33. *Id.*

34. Data Retention (EC Directive) Regulations, 2007, S.I. 2199, art. 10, ¶ 1 (U.K.); Goodall, *supra* note

15.

35. Anti-Terrorism, Crime and Security Act, 2001, c. 24, Part 11 (U.K.), *available at* http://www.opsi.gov.uk/acts/acts2001a.

36. Goodall, *supra* note 15.

37. *Id.*

38. Data Retention (EC Directive) Regulations, 2007, S.I. 2199, art. 10, ¶ 2 (U.K.); Goodall, *supra* note 15.

39. Bird & Bird: Privacy & Data Protection Group, Implementation of EC Data Retention Directive (2006/24), June 28, 2007, http://www.twobirds.com/English/News/Articles/Pages/Implementation_EC_Data_Retention_Directive.aspx .

40. Karin Retzer, Of Counsel, Morrison Foerster, *Data Retention: Denmark Is First EU Member State to Implement Controversial Directive* (May 4, 2007), http://www.mofo.com/news/updates/bulletins/12271.html.

41. Rodney Petersen, *Toward a U.S. Data-Retention Standard for ISPs*, EDUCAUSE REV., Nov./Dec. 2006, at 78–79 (internal citation omitted), *available at* http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume41/TowardaUSDataRetentionStandard/158105 .

42. U.S. Internet Service Provider Association, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945, 947 (2003).

43. Joel Micheal Schwarz, *'A Case of Identity:' A Gaping Hole in the Chain of Evidence of Cyber-Crime*, 9 B.U. J. SCI. & TECH. L. 92, 100-01 (2003).

44. 18 U.S.C. § 2703(d) (2006).

45. Monique Mattei Ferraro, *The States and the Electronic Communications Privacy Act: The Need for Legal Processes that Keep Up with the Times*, 22 J. MARSHALL J. COMPUTER & INFO. L. 695, 700 (2004).

46. *Id.*

47. Schwarz, *supra* note 43, at 101.

48. *Id.* at 101-02.

49. 18 U.S.C. § 2703 (2006).

50. United States Internet Service Provider Association, The US Data Preservation System: Title 18 U.S.C. Section 2703(f), http://www.usispa.org/pdf/DataPreservationSystem.pdf (last visited Sept. 21, 2009).

51. *Id.*

52. Declan McCullagh, *Gonzales Pressures ISPs on Data Retention*, CNET NEWS, May 26, 2006, http://www.news.com/Gonzales-pressures-ISPs-on-data-retention/2100-1028_3-6077654.html?

tag=nl.

53. Jon Swartz & Kevin Johnson, *U.S. Asks Internet Firms to Save Data*, USA Today, June 1, 2006, http://www.usatoday.com/tech/news/Internetprivacy/2006-05-31-Internet-records_x.htm%5C.

54. Jason M. Young, *Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation—A Critical Analysis of the Council of Europe Convention on CyberCrime & the Canadian Lawful Access Proposal*, 7 Yale J. L. & Tech. 346, 374 (2005), *available at* http://www.yjolt.org/files/young-7-YJOLT-346.pdf.

55. *Id.* at 375 (discussing 18 U.S.C.A. § 2703(c)(2) (West 2003)).

56. Department of Justice, Computer Crime and Intellectual Property Section: Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last visited Nov. 18, 2008).

57. 18 U.S.C. § 2706(a) (2006).

58. 18 U.S.C. § 2706(b) (2006).

59. 18 U.S.C. § 2706(a) (2006).

60. U.S. Internet Service Provider Association, *supra* note 42, at 970.

61. See Goldberg, *supra* note 9 (observing that "The Directive has been transposed into UK law by the Data Retention Regulations 2007, which came into force on October 1, 2007.").

62. Int'l Chamber of Commerce et al., Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes (2003), *available at* http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/Common_Industry_Statement_on_Storage_of_Traffic_Data_June03.pdf. Additional organizations that support the statement include the Union of Industrial and Employers' Confederations of Europe ("UNICE"), European Information, Communications and Consumer Electronics Technology Industry Association ("EICTA"), and International Telecommunication Users Group ("INTUG").

63. *Id.*

64. *See* Home Office, The Initial Transposition of Directive 2006/24/EC: Government Responses to the Consultation (2007) (U.K.), http://www.homeoffice.gov.uk/documents/euro-directive-retention-data/cons-responses-07-euro-directive?view=Binary.

65. *Id.*

66. *Id.*

67. *Id.*

68. Google has stated that it retains its identifiable search records for 18 to 24 months. Patrick Mueller, *Legal Brief: Will the Feds Run Your Log Servers*, Network Computing, Apr. 16 2007, http://www.networkcomputing.com/immersion/dataprivacy/showArticle.jhtml?articleID=198900106. While search data is not covered by the Directive, the fact that companies already have mechanisms for retaining data, or have established methods for complying with the European

Union's Directive, would likely result in a lower cost if the United States implemented a data retention law.

69. *Cf. Software Piracy: BSA or Just BS?*, ECONOMIST, May 19, 2005 (discussing how the Business Software Alliance statistics, in connection with software piracy, were exaggerated).

70. Davies & Trigg, *supra* note 24.

71. Young, *supra* note 54.

72. *See* Declan McCullagh, *GOP Revives ISP-tracking legislation*, CNET NEWS, Feb. 6, 2007, http://www.news.com/GOP+revives+ISP-tracking+legislation/2100-1028_3-6156948.html; *see also* Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2007, H.R. 837, 110th Congress § 6 (2007), *available at* http://thomas.loc.gov/home/gpoxmlc110/h837_ih.xml.

73. The Obama administration has yet to state its position with regard to enacting a data retention law.

74. *See* H.R. 837.

75. For example, switching from data preservation to data retention means the government no longer needs to request to retain personal information. Moreover, new requirements may also give rise to violations of the First Amendment. *See, e.g.*, Catherine Crump, Comment, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 196-97 (2003).