KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

DATA RETENTION MANDATES: A THREAT TO PRIVACY, FREE EXPRESSION AND BUSINESS DEVELOPMENT

OCTOBER 2011

I. Introduction

A. What is data retention?

The providers of telecommunications and Internet services collect and store a wealth of data about their customers. This information varies depending on the service and the business model of the provider, but it may include subscriber identifying information, assignments of Internet addresses to individual users, location information about mobile devices, Internet connection and browsing data, telephone dialing records, and other addressing, signaling or routing information, often time-stamped and often capable of being associated with a particular user. (The data indicating usage is sometimes referred to as traffic data, meta-data, or transactional data.) Government officials around the world have long demanded that service providers disclose this information for use in criminal or national security investigations, under authorities and standards that vary depending on national law.

In recent years, however, some governments, not satisfied with the amount of information that service providers collect and retain in the ordinary course of business, have imposed or considered imposing legal mandates requiring service providers to retain certain data about all of their users for specified periods of time, even when that data no longer is needed for a business purpose. Generally, under these mandates, the data must be collected and stored in a manner such that it is linked to users' names or other identification information. Government officials may then request access to this data, pursuant to the laws of their respective countries.

The Council of Europe's Convention on Cybercrime[1] takes a different approach. Countries signing the COE Convention must adopt laws authorizing government officials to demand that a communications service provider *begin, upon receipt of a specific request,* to store – "preserve" – data about a specific user or device relevant to a specific criminal investigation or proceeding. Typically, the service

[1] Signatories to the Convention on Cybercrime include 43 of the member states of the Council of Europe, Canada, Japan, South Africa, and the US. However, the US is the only non-European state to have actually ratified the Convention. *See Council of Europe: Convention on Cybercrime,* Apr. 16, 2011, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

provider is required to continue preserving this data for up to a maximum period of time, such as 90 days, while the government agents obtain the necessary authorization to compel its disclosure. This process is known as *data preservation* and is discussed toward the end of this paper as a response to governmental interests that is preferable to data retention.

B. Why do countries adopt data retention laws?

To some extent, particularly in Europe, data retention mandates emerged as a reaction to data destruction mandates. The 1995 European Union directive on data protection requires commercial entities, including ISPs, telephone companies and other communications service providers, to delete data when it is no longer necessary for a business purpose.[2] In the case of free services, this may prohibit companies from holding data for any period of time. After this data destruction mandate was implemented in Europe, law enforcement and national security agencies, if they were slow in their investigations, sometimes found that data identifying the sender of a communication or revealing a suspect's associates or movements was no longer available when they asked for it. At the same time, government investigators began to appreciate that digital technology was becoming woven into people's daily lives, generating a wealth of highly revealing information, and that those services could be designed or programmed to generate even more information, to store it, and make it retrievable and useful. Even in the absence of a data destruction mandate, governments began to realize that they could demand that companies collect and keep even more data for even longer periods of time.

In this context, the immediate trigger for adoption of data retention mandates is often some crisis or some especially sensational type of crime. Following the attacks of September 11, 2001, for example, the UK passed the Anti-Terrorism Crime and Security Act 2001, which established a framework for a "voluntary" data retention regime for telecommunications companies.[3] The 2004 Madrid bombings and the 2005 London bombings led the European Union to adopt Directive 2006/24/EC, known as the Data Retention Directive (DRD).[4] In the US, the Department of Justice recently (and so far unsuccessfully) has called for a data retention law to facilitate child pornography investigations.[5]

C. What problems do data retention laws create?

Generally, data that is retained pursuant to a mandate will be available to the government not only for the purpose that triggered adoption of the mandate but also for other crimes and for national security investigations. Moreover, data compiled in pursuit of legitimate goals can be

---

[2] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[3] Home Office, *Retention of communications data under Part 11: Anti Terrorism Crime and Security Act 2001 – Voluntary Code of Practice*, Jan. 2004, (UK).

[4] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT [hereinafter EU DRD]. See Claire Walker, *Data retention in the UK: Pragmatic and proportionate, or a step too far?*, 25 COMPUTER LAW & SECURITY REVIEW 325-334 (2009).

[5] Declan McCullagh, *DOJ Wants Mandatory Data Retention,* CBS NEWS, Jan. 25, 2011, http://www.cbsnews.com/8301-501465_162-20029440-501465.html.

abused.[6] In Poland, for example, in 2010, the press reported that government agents had abused the country's data retention law: as part of a politically motivated plot, agents accessed mobile phone location and traffic data stored under the country's data retention law and compiled lists of high-profile journalists' sources.[7] In Thailand, the country's Computer Crimes Act (CCA) has been used to prosecute web forum moderators and bloggers.[8] In one especially high-profile case prosecuted under the CCA, law enforcement arrested a website moderator and used the information she had been required under law to retain to locate, arrest, and charge one of the anonymous posters to her website. The charge? Disparaging the king.[9]

Even where law enforcement access to retained data is appropriately limited by structural and legal mechanisms, data retention laws create risk of other significant harms. These harms are discussed in greater detail in this paper, but are summarized below:

- Data retention, because of the resource constraints it places on companies and because it increases the ratio of low-value data to high-value data, may ultimately hinder law enforcement's ability to access the information it needs in a timely manner, especially in emergency situations.
- Data retention, by creating records that link highly detailed descriptions of users' Internet activity to identifying information, violates fundamental human rights, such as the right to privacy, the right to freedom of expression, and the right to the presumption of innocence.
- Data retention increases the risks of damaging data breaches and identity theft.
- The financial cost of data retention can inhibit growth and innovation in the ICT industry, particularly by making it hard for new companies to launch.

An alternative to data retention is data preservation, which avoids the risks inherent in data retention and is discussed in detail toward the end of this paper.

II. Data Retention: The Basics

Data retention laws vary considerably with respect to the types of data, companies, and activities that they impact.

---

[6] *See e.g.,* examples included in AKVORRAT, THERE IS NO SUCH THING AS SECURE DATA: REFUTING THE MYTHS OF SECURE IT SYSTEMS at 26-37, http://www.wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

[7] Wojciech Czuchnowski, *Dziennikarze na celowniku służb specjalnych [Journalists Targeted by Special Forces]*, GAZETA WYBORCZA (Poland), Oct. 8, 2010; Letter from the Helsinki Foundation for Human Rights to Donald Tusk, Prime Minister of Poland (Oct. 13, 2010), https://www.bof.nl/live/wp-content/uploads/Premier_HFPC_specs%C5%82u%C5%BCby_13.10.2010_eng.pdf; *Surveillance of Polish Journalists Case – New Developments,* HUMAN RIGHTS HOUSE (Jan. 14, 2011).

[8] Sinfah Tunsarawuth and Toby Mendel, *Analysis of Computer Crime Act of Thailand* (May 2010), http://thainetizen.org/sites/default/files/Analysis%20of%20Computer%20Crime%20Act%20of%20Thailand%20By%20Sinfah%20Tunsarawuth%20and%20Toby%20Mendel.pdf.

[9] *Id.* at 18.

A. Types of companies enlisted

Most of the data retention laws that have been adopted focus on Internet service providers (ISPs); the term "ISP" can encompass both traditional cable or DSL access providers and mobile providers, although data retention laws are often not clear on this point. Some data retention laws go much further and apply to any entity that offers Internet access, such as coffee shops, WiFi "hotspots," libraries, or companies whose employees use the Internet at work.[10] Some data retention laws are unclear about whether or not they apply to these access-point providers.

Some data retention laws place retention obligations on a third category of entities, known as online service providers (OSPs). OSPs provide web-hosting services, email services, hosting services for user-generated content, and mobile and web applications. Video-hosting sites, social networking platforms, blogging platforms, and mobile "apps" are all OSPs. France, for example, requires that web hosting and online payment service providers retain identity-linked data about users (as well as their passwords) for at least one year.[11] Some laws – or the government-issued regulations that describe how they should be implemented – have created considerable confusion about the extent to which they apply to online service providers.

B. Types of data retained

The types of data that must be retained under data retention laws vary considerably from country to country.

1. Retention of IP address allocations

Under the narrowest definition, "data retention" can refer to the retention of IP ("Internet Protocol") address allocation records by ISPs. In general, every time a device is connected to the Internet, it is assigned an IP address. ISPs issue these addresses to their customers. A log of these address allocations will indicate which device was assigned which IP address for a particular period of time. In the simplest configuration of Internet access, the IP address of origination is associated with a particular communication as it is transmitted through the Internet.

For common residential broadband Internet access, each customer's household is assigned an IP address whenever the household turns on its service. This IP address can remain the same for days or weeks, but it can change, both on a regular schedule and whenever the hardware in the household is turned off or loses power. This use of "dynamic IP addresses" is an efficient and effective way for an ISP to manage its service. A consequence of dynamic IP addresses, however, is that the person who is communicating using a given IP address on one day may not be the person who was using that same IP address last week or last month.

---

[10] *See* e.g., Thailand's Computer Crime Act and India's Information Technology (Amendment) Act of 2008. *See* Computer Crime Act BE 2550 (2007), Vol 124, Section 27 Kor, *Government Gazette,* 18 June 2007 (Th.), unofficial translation available at http://www.prachatai.com/english/node/117 [hereinafter CCA—Thailand]; The Information Technology (Amendment) Act, 2008 (No. 10 of 2009)(In.), *available at* http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf [hereinafter ITA—India].

[11] Decree No. 2011-219 of Feb. 25, 2011, Journal Officiel de la Republique Francaise [J.O.][Official Gazette of France], Mar. 1, 2011, p. 3643, *available at* http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000023646013&dateTexte=&oldAction=rechJO&categorieLien=id. *See also French Decree Establishes What Data Must be Retained by Hosting Providers,* EDRI-GRAM No. 9.5, Mar. 9, 2011, http://www.edri.org/edrigram/number9.5/data-retention-hosting-france.

Moreover, the actual practice of network configuration is often much more complicated than described above. The IP address that is passed through the network may not actually be unique to a specific end user or end-user device. In some cases, the address may merely identify the access point: the coffee shop or university, for example. Such access points may have many users, each of whom is not uniquely identified higher up in the network. In other instances, ISPs use a system called carrier-grade Network Address Translation (NAT), which stands between the upstream network and many, often thousands, of customers. In such cases, the IP address that is passed through the network only identifies the network component serving that subset of the provider's users. In these systems, it is difficult to associate individual users with the IP addresses that are passed through the network.[12]

The reality is further complicated in the context of mobile Internet access, where different addresses may be assigned to a single device many times during the course of a day. In some mobile configurations, as in some non-mobile configurations, the address passed through the network with a communication may not be uniquely associated to a specific end-user device. Policymakers proposing data retention mandates are often not aware of these complexities. And ensuring end-user identity with these complexities would require much broader laws, imposing much more extensive recordkeeping requirements on a much broader range of entities.[13]

2. Retention of traffic data

Under some data retention laws, ISPs, access-point providers, and online service providers that provide communications services such as webmail or VOIP[14] are required to record the traffic data of individual users. Traffic data may include addressing or routing information, information concerning the identities and locations of the users involved in a communication, the duration, type, and volume of communications, and information about the type of network or equipment used. Under some laws, traffic data includes URL browsing information, and in other cases it does not.[15]

---

[12] For more information about Natural Address Translation, *see* Cisco, How NAT Works: Document ID 6450 (March 29, 2011), http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml.

[13] All of this is only going to get more complicated with the roll-out of IPv6. IPv6 privacy addresses, which are turned on by default in Windows, refresh every 24 hours under the default configuration. Furthermore, many ISPs are going to be rolling out large-scale network address translation (NAT) devices to manage the transition from IPv4 to IPv6. This means that many more users will be sharing public-facing IPv4 addresses and under a data retention mandate, ISPs would need to store more information about how they do address assignment, including not only IP addresses but also port numbers. Any data retention mandate that does not account for these changes will become outdated in the near future, and yet accounting for the changes is quite difficult since there are a large number of IPv6 transition technologies and configurations, each of which may require a different set of data to be retained.

[14] In Europe, there has been widespread disagreement about whether the Data Retention Directive applies to services such as webmail and VOIP. *See e.g., Commission Report of the Data Retention Conference, 'Toward the Evaluation of the Data Retention Directive,'* COM (May 14, 2009), *available at* http://ec.europa.eu/home-affairs/doc_centre/policeT/docs/meeting_report_09_07_14_en.pdf.

[15] In Europe, for example, traffic data does not include URLs while in Thailand it does. *See* Press Release, Article 29 Data Protection Working Party, European Data Protection Authorities Find Current Implementation of Data Retention Directive Unlawful (Jul. 14, 2010), http://ec.europa.eu/justice/policies/privacy/news/docs/pr_14_07_10_en.pdf) [hereinafter WP29 Press Release]; Annex Notification of the Ministry of Information and Communication Technology Re: Criteria concerning Archiving of Computer Traffic Data of Service Provider B.E. 2550; Tim Bass, Slideshow from Presentation to the AMCHAM ICT Committee & Internet Service Providers on the Computer Crime Act B.E. 2550(2007) & Ministry of ICT Notification, 2008, http://www.slideshare.net/TimBassACIS/computer-crime-act-be-2550-2007-ministry-of-ict-notification-presentation.

While traffic data does not include the content of communications – the text of an email, for example – it still contains highly sensitive information. In the words of the European Commission's Article 29 Data Protection Working Party:[16]

> [T]he availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users' private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression. … [T]he mere availability of traffic data…allows tracing several items of personal information related to data subjects (including sensitive information) based on the overall picture (e.g. behavioural profiles of individual users) that can be derived of their social interactions.[17]

3. Retention of location data

Sometimes "location data" is subsumed under the traffic data category, other times it is treated separately. Location data can refer to the physical location of the connected computer or to the geographic location of a mobile phone (derived from the cell tower to which it is connected at any given moment). For users of mobile phones, location data can prove especially sensitive, because it provides a very detailed picture of a person's movements. For example, before Germany's data retention law was overturned by the Federal Constitutional Court, Deutsche Telekom, pursuant to law, stored the latitude and longitude associated with each user's smart phone each time it checked email.[18]

4. Retention of the content of communications

Data retention laws generally do not require covered entities to retain the content of communications. The EU DRD, for example, prohibits retention of content data.[19] However, India is in the process of deciding whether its data retention law will apply to traffic data alone or also to content data, such as the content of emails and instant messages. Also, in Europe, a review of country-specific transpositions of the Data Retention Directive by the European Commission's Article 29 Data Protection Working Party found that ISPs were illegally and regularly retaining information such as website URLs and headers of e-mail messages (information that the EU does not consider traffic information).[20] This finding suggests that requiring ISPs to retain traffic data may also lead to the retention of content data as well.

---

[16] The Article 29 Data Protection Working Party was established by the European Commission under Article 29 of the Data Protection Directive to offer expert advice on data protection to member states and to the Commission.

[17] Article 29 Data Protection Working Party, Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, (July 13, 2010) at 6, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf [hereinafter WP29].

[18] *See* Tell-all Telephone Interactive Display, ZEIT ONLINE, http://www.zeit.de/datenschutz/malte-spitz-data-retention (last visited Oct. 6, 2011).

[19] EU DRD Art. 1, Section 2. *See also* EU DRD Recital 13.

[20] WP29 at 9.

C. Length of retention period

The "retention period" refers to the length of time for which companies are required to store user data. In Thailand, the law requires retention for at least 90 days.[21] In the EU, the DRD instructs member states to implement laws that specify retention periods between six months and two years.[22] The Indian government is in the process of determining the retention period for entities affected by the Indian Telecommunications Act. In Argentina, the announcement of a ten-year retention period was met with such outrage by citizens and industry that the law was immediately suspended.

D. Financial burden

Data retention laws may place financial burdens on industry and on government. Data retention requires investment in data storage centers, systems that make the data easy to retrieve upon government request, and technical expertise for maintaining these systems. Some governments place the entire cost burden on ICT companies, while others provide some type of relief for certain costs. [23] Governments that do not provide relief for costs associated with responding to law enforcement requests for information have little financial incentive to control the number of such requests.

E. Restrictions on access to retained data

Proposals to mandate data retention cannot be viewed in a legal vacuum but rather must be considered in light of the privacy protections that are afforded the data held by service providers. These privacy protections can be of two types: protections that limit access by government and protections that limit access by private entities.

In all countries, questions arise around the conditions under which law enforcement can gain access to retained data. Some data retention laws may seek to limit access only to investigations of specified crimes. For example, the EU DRD generally limits access by law enforcement to that necessary for the "investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."[24] (The Directive, however, does not provide a definition of "serious crime.") A separate question is the source of authority and the threshold of justification, if any, that must be met for access. Such standards vary considerably. In some counties, including the U.S., government agents can demand access to traffic data without judicial approval. In the U.S. and other countries, standards for access in national security cases may be especially weak.

Data retention laws must also be evaluated in the context of laws governing commercial access to and use of retained data. In Europe, where data retention mandates first arose, there are relatively strict privacy protections on commercial data in general. Moreover, in Europe,

---

[21] CCA—Thailand, Section 26.

[22] EU DRD Art. 6; *See also* this chart listing the retention periods established by those: EU member states who have transposed the directive: WP29 Report, Annex, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_annex_en.pdf.

[23] *Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC),* COM (2011) 225 final (Apr. 18, 2011) at 27, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

[24] EU DRD Art.1.1.

companies are specifically prohibited from using for commercial purposes data retained pursuant to the DRD.[25] In contrast, when evaluating a proposed data retention law, the National Human Rights Commission of Korea stated that the country's weak commercial privacy law gave cause for a heightened level of concern about the privacy violations that would be created by data retention.[26] In India, which lacks a baseline consumer privacy law, questions have been raised about whether ISPs will seek to subsidize the costs of soon-to-be-implemented data retention requirements by using retained data for marketing purposes.[27]

F. The volume of data mandated to be retained – and subsequently disclosed to government officials – can be enormous

The volume of data stored under retention mandates is astonishing. For example, in Germany, Deutsche Telekom stored location data on its mobile users pursuant to the German transposition of the DRD (before the transposition was struck down by the Federal Constitutional Court).[28] The data for just one user included 35,831 data points –over a six-month period, revealing attendance at political events as well as personal activity.[29] In 2009, Danish ISPs reported that in order to comply with the country's transposition of the DRD, they collected 450 billion data records, an average of 82,000 data records for every Dane.[30] And when the data exists, government officials can become profligate in requesting it. In 2009, the Polish government issued one million requests for access to data retained under the nation's transposition of the DRD; this amounts to one request per every 38 citizens.[31] That same year, the government in the Czech Republic requested access to retained data 280,000 times, amounting to one request per every 37 citizens.[32]

III. Risks Posed by Data Retention Mandates

A. Data retention laws may hinder law enforcement efforts

In testimony before the US Congress, the US ISP Association explained that requiring service providers to store large volumes of data may actually hinder law enforcement's ability to access the information it needs in a timely fashion. Large-scale data storage increases the likelihood of

---

[25] *See e.g.,* EU DRD, Recitals 3, 14, 12, and 15.

[26] Press Release, National Human Rights Commission of Korea, NHRCK Announces Opinion on Proposed Amendments to the Protection of Communications Secrets Act (Jan. 30, 2008), http://www.humanrights.go.kr/english/activities/view_01.jsp?seqid=713&board_id=Press%20Releases.

[27] *See* Sunil Abraham, *Does the Government want to enter our homes?*, THE CENTRE FOR INTERNET & SOCIETY INTERNET GOVERNANCE BLOG, Aug. 13, 2010, http://www.cis-india.org/advocacy/igov/blog/government-enter-homes.

[28] Noam Cohen, *Cellphones Track Your Every Move, and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html.

[29] Tell-all Telephone Interactive Display, ZEIT ONLINE, http://www.zeit.de/datenschutz/malte-spitz-data-retention (last visited Oct. 6, 2011).

[30] Thomas Breinstrup, *Dommere siger nej til EU-overvågning* [Judges Say No to EU Monitoring], BUSINESS.DK, Mar. 2, 2010, http://www.business.dk/tech-mobil/dommere-siger-nej-til-eu-overvaagning.

[31] *Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC),* COM (2011) 225 final (Apr. 18, 2011) at 40, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

[32] *Id.*

system crashes and failures; the greater the volume of stored data, the less reliable the integrity of the data and the longer the delays when ISPs respond to requests from law enforcement. The biggest concern is that responses in true emergencies will be delayed because the more data there is, the longer it will take to search through it and find what is relevant.[33]

Long retention periods result in longer and more frequent delays but for little relative gain: the older the data, the less useful it is for law enforcement. A study by the European Commission showed that in 2008, 75% of the retained Internet traffic data requested by law enforcement was less than six months old and 93% was less than a year old.[34]

B. Data retention laws violate fundamental human rights

For sixty years, international human rights law has enshrined the rights to freedom of expression, access to information, privacy of communications, and the presumption of innocence, creating a strong bias against government intrusions into these rights. These rights are reflected both in the provisions of numerous international and regional agreements and in decisions rendered by human rights tribunals.[35]

Central to free expression and the protection of privacy is the right to express beliefs – even controversial beliefs – without fear of retribution. Historically, one way to do this has been to publish anonymously (or pseudonymously). The importance of anonymity online has been widely recognized. In the U.S., federal and state courts have found that the Constitution protects the right to speak anonymously on the Internet.[36] In Europe, the Council of Europe's 2003 "Declaration of freedom of communication on the Internet" states that "to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity."[37] The European Commission's Article 29 Working Party has argued that the "ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their

[33] Written Testimony of Kate Dean (United States Internet Service Provider Association) before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism and Homeland Security on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," Jan. 25, 2011, http://judiciary.house.gov/hearings/pdf/Dean01242011.pdf (hereinafter US ISPA Testimony).

[34] *Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC),* COM (2011) 225 final (Apr. 18, 2011) at 22, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

[35] *See e.g.,* The Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (art. 6.2), UDHR (art 11). For a more detailed discussion of this topic *see* CENTER FOR DEMOCRACY & TECHNOLOGY, "REGARDLESS OF FRONTIERS:" THE INTERNATIONAL RIGHT TO FREEDOM OF EXPRESSION IN THE DIGITAL AGE, VERSION 0.5 – DISCUSSION DRAFT (Apr. 2011), http://www.cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf.

[36] For example, *Solers, Inc. v. Doe*, 2009 D.C. App. LEXIS 342 (D.C. Cir. 2009); *Doe v. Cahill*, 884 A.2d 451 (Del. 2005); *Doe v. 2TheMart.com*, 140 F. Supp. 2d 1088, 1092, 1095 (W.D. Wash. 2001).

[37] Of course, this freedom "does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts," in accordance with national laws and other international conventions and agreements. Declaration on Freedom of Communication on the Internet (Adopted by the Committee of Ministers, May 28, 2003), https://wcd.coe.int/ViewDoc.jsp?Ref=Decl-28.05.2003.

privacy on-line as they currently enjoy off-line."[38] Internationally, the UN Special Rapporteur on Freedom of Opinion and Expression has emphasized the importance of anonymity online.[39]

Data retention laws obliterate the right to anonymous speech and thereby fundamentally violate users' rights to privacy and free expression as well as the presumption of innocence.

These human rights concerns are not theoretical. At least one study has shown that data retention in Europe has significantly diminished citizens' willingness to discuss and obtain information about mental health issues online.[40] In Poland, intelligence agencies used data stored under the country's data retention law to expose information about journalists' sources.[41]

Human rights institutions that have taken up data retention mandates have found that they infringe on human rights. The European Commission's Article 29 Working Party assailed data retention, stating, "it encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish."[42] In 2008, the National Human Rights Commission of Korea, an independent governmental body charged with analyzing laws from a human rights perspective, expressed deep concern over proposed amendments to South Korea's Protection of Communications Secrets Act that would have created three to twelve-month data retention requirements for location data, traffic data, and certain content data.[43] The Commission held that such an amendment contradicted the principle of data minimization as well as service providers' obligations to protect personal information. Acknowledging law enforcement's legitimate interest in investigating crime, it wrote:

> However, requiring telecommunication service providers to keep communication records of ordinary persons for up to one year for the purpose of resolving crimes which have not occurred yet, not even at the stage of preparing for crimes, is…highly likely to infringe upon human rights…[and] there exists a high possibility that personal information may be leaked and abused for a long

[38] Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, "Recommendation 3/97: Anonymity on the Internet," Dec. 3, 1997, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf.

[39] Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/7/14, Paras. 71, 24, Feb. 28, 2008, http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/7/14&Lang=E.

[40] *See* Axel Arnbak, Plenary Presentation at the Taking on the Data Retention Directive Conference in Brussels: What the European Commission Owes 500 Million Europeans (Dec. 3, 2010) at 3, *available at* http://www.edri.org/files/Data_Retention_Conference_031210final.pdf (find that as a result of data retention, "half of Germans will not contact marriage counselors and psychotherapists" via e-mail), citing a German-language study by FORSA, "Opinions of citizens on data retention," June 2, 2008, *available at* http://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf.

[41] *See* note 7 above; *see also* Axel Arnbak, Plenary Presentation at the Taking on the Data Retention Directive Conference in Brussels: What the European Commission Owes 500 Million Europeans (Dec. 3, 2010), *available at* http://www.edri.org/files/Data_Retention_Conference_031210final.pdf.

[42] WP29 at 4.

[43]ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULES IN CYBERSPACE (Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain eds., MIT Press, 2010) at 503, *available at* www.access-controlled.net/wp-content/PDFs/part2/028_South%20Korea.pdf.

time…[44]

In Europe, national courts have found national transpositions of the EU DRD to be unconstitutional violations of fundamental human rights. For example, Germany's Federal Constitutional Court annulled the country's transposition of the DRD; the court's president noted that data retention can "cause a diffusely threatening feeling of being under observation that can diminish an unprejudiced perception of one's basic rights in many areas."[45] The Czech Constitutional Court held that its country's implementation of the Directive "does not meet the requirements arising from the rule of law and is in conflict with demands to limit the fundamental right to privacy in the form of a right to informational self-determination."[46]

In rejecting data retention mandates, courts have consistently emphasized that such mandates sweep in every citizen, whether or not these citizens have committed a crime or are engaging in protected speech. As the Romanian Constitutional Court wrote when it invalidated the country's transposition of the DRD: "data retention itself is likely to overturn the presumption of innocence and to transform *a priori* all users of electronic communication services or public communication networks into people suspected of committing terrorism crimes or other serious crimes."[47]

Under international law, a key concept in judging the validity of any restriction on protected rights is whether the restriction is "necessary" to serve a legitimate government interest, a judgment that entails an inquiry into the proportionality and effectiveness of the restriction.[48] Data retention laws fail these tests. By infringing on the rights to free expression and privacy of all citizens – and reversing the presumption of innocence for all citizens – these laws are far from proportional. Indeed, the Romanian, German, and Czech Constitutional Courts held that their nation's data retention mandates violated the principle of proportionality. Furthermore, the effectiveness of data retention laws as tools to fight crime has not been established; indeed, ISPs have noted that data retention mandates may make it *more* difficult for them to cooperate with law enforcement.

---

[44]Press Release, National Human Rights Commission of Korea, NHRCK Announces Opinion on Proposed Amendments to the Protection of Communications Secrets Act (Jan. 30, 2008), http://www.humanrights.go.kr/english/activities/view_01.jsp?seqid=713&board_id=Press%20Releases.

[45] Bundesverfassungsgericht [BVerfG][Federal Constitutional Court] Mar. 2, 2010, 1 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 256/08 (F.R.G.), *available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html*; Judy Dempsey, *German Court Orders Stored Telecom Data Deleted,* N.Y.TIMES, Mar. 2, 2010, *available at* http://www.nytimes.com/2010/03/03/world/europe/03iht-data.html.

[46] Nález Ústavního soudu (Czech Republic Constitutional Court) cj. 24 / 2010 / Sbírka nálezu a usnesení Ústavního soudu (Collection of Court Decisions of the Constitutional Court) (Czech Rep.), *available at* http://www.concourt.cz/clanek/GetFile?id=5075; Press Release, Constitutional Court of the Czech Republic, Ústavní Soud Zrušil Část Zákona o Elektronických Komunikacích [Constitutional Court Struck Down Part of the Electronic Communications Act] [in Czech, with link to the decision] (Mar. 31, 2011) *available at* http://www.concourt.cz/clanek/5068.

[47] Decision no.1258, Romanian Constitutional Court, Oct. 8, 2009. Published in the Romanian Official Monitor, no. 789, Nov. 23, 2009. English translation (unofficial): http://www.legiinternet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.

[48] *See* discussion in CENTER FOR DEMOCRACY & TECHNOLOGY, "REGARDLESS OF FRONTIERS:" THE INTERNATIONAL RIGHT TO FREEDOM OF EXPRESSION IN THE DIGITAL AGE, VERSION 0.5 – DISCUSSION DRAFT (Apr. 2011), http://www.cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf.

C. Data retention laws create new privacy risks

A fundamental principle of privacy protection is data minimization: to protect user privacy, the amount of data collected and held by entities should be minimized.[49] Data retention laws undermine this important principle by requiring that companies maintain large databases of information that is not needed for a business purpose. This retained data is then vulnerable to hackers, accidental disclosure, and other unauthorized third-party access, thereby aggravating the identity theft problem.[50] And the longer data is maintained, the more at risk it is to compromise or disclosure. The risk of harm is even greater when entities that have not traditionally kept data on their customers – such as coffee shops, airports, libraries, Internet cafes, and others offering wireless access – are required to keep information on customers who use wireless services.

Existing implementations of data retention mandates indicate that educating companies about these risks and obtaining compliance with security requirements are not simple. For example, in an evaluation of individual countries' implementations of the EU DRD, the European Commission's Article 29 Working Party reported that "there appears to be no standard awareness of the risks related to traffic data retention."[51] The evaluation found the largest security gaps in the practices of smaller providers; the high cost of implementing security rendered these providers "unable to implement top IT security solutions protecting the traffic data to the same degree of complexity as the industry leaders[.]"[52] Smaller providers are also engaging in widespread outsourcing of retention requirements, a practice that has made it more difficult to evaluate whether they are effectively complying with data protection requirements.[53] The Working Party additionally identified a separate, yet equally consequential, security failure: even where data is held in a secure fashion, many companies fail to transmit it to law enforcement using secure procedures.[54]

Once retained pursuant to a data retention mandate, there is also a real risk that data may also be put to other legal, but privacy-invasive uses. For example, service providers, once they are forced to invest in building databases of customer information, may decide to repurpose that data for other uses, such as behavioral advertising.

D. Data retention laws impose costs on businesses, inhibiting innovation and limiting access to ICTs

Data retention laws diminish competition and innovation, harming consumers and industry, including small businesses.

---

[49] *See* The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[50] WP29 at 6 ("[I]mplementation of the [Data Retention] directive by electronic communications and Internet service providers is associated with an inherently high risk level such as to require appropriate technical and organisational security measures.").

[51] WP29 at 12.

[52] *Id* at 12.

[53] *Id* at 17-18.

[54] *Id* at 14.

A threshold concern is cost. By definition, a data retention law requires companies to store data that they have no business reason to retain.[55] Unless government is willing to cover the capital and operating costs associated with data retention compliance, the extra costs fall on the covered providers.[56] Europe's ISP trade association (EuroISPA) has identified a long list of key capital costs and operating costs associated with data retention compliance. Capital costs include the costs of: system design, collection and storage equipment, integration of new and existing system, and systems to identify and deliver requested data to law enforcement in a timely manner. Key operating costs include the costs of access procedures and security (to distinguish between legitimate and illegitimate requests for data), compliance implementation staff, law enforcement liaison staff, staff training, system maintenance, and continuing integration costs.[57]

European ISPs have produced widely varied calculations of capital and operating costs, likely reflecting differences in expected levels of government reimbursement, business size, retention periods, and the frequency of government requests for data.[58] For example, the Dutch ISP KPN calculated that retention of Internet data would require a one-time investment of 5 million Euros and yearly operational expenditures of 4 million Euros.[59] The Dutch senate estimated a total initial national investment of 75 million Euros followed by an annual expenditure of 12-20 million Euros.[60] The Portuguese ISP Sonaecom estimated that capital costs would be 500,000 Euros.[61] Austria estimated that data retention-related capital costs for the country as a whole would be 15-20 million Euros and that annual operating costs would run around 3 million Euros.[62] German telecommunications companies estimated that they invested 300 million Euros alone on equipment purchases required to implement the Directive.[63]

---

[55] *See* e.g., US ISPA Testimony; Cable & Wireless, Response to the Commission Questionare to the Private Sector in Relation to the Implementation of the Data Retention Directive (Austria, Belgium, France, Germany, Italy, Ireland, Netherlands, Spain, Switzerland) (Nov. 2009) *available at* https://www.vorratsdatenspeicherung.de/images/DR-consult/csp_cable&wireless.pdf; Online Safety and Technology Working Group (OSTWG),Youth Safety on a Living Internet (Jun. 4, 2009) at 102, *available at* http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_ 060410.pdf.

[56] Cable Europe, GSMA Europe, EuroISPA, ECTA (European Competitive Telecommunications Association), and ETNO (The European Telecommunications Network Operators' Association), Data Retention: Impact on Economic Operators (2009) at 1-2, *available at* https://www.vorratsdatenspeicherung.de/images/DR-consult/csp_joint_statement.pdf [hereinafter EU Joint Industry Statement].

[57] *Commission Report of the Data Retention Conference, 'Toward the Evaluation of the Data Retention Directive,'* COM (May 14, 2009) at 7-8, *available at* http://ec.europa.eu/home-affairs/doc_centre/police/docs/meeting_report_09_07_14_en.pdf.

[58] *See* submissions available at https://www.vorratsdatenspeicherung.de/images/DR-consult/. *See also* EU Joint Industry Statement at 1-2.

[59] KPN Netherlands, Answers to EC Questionnaire on Data Retention Directive (2009), *available at* https://www.vorratsdatenspeicherung.de/images/DR-consult/csp_kpn.pdf.

[60] *Officials, ISPs Meeting Sparks Debate Over New Law's Data Retention Obligations,* 26 October 2009, *available at* http://news.bna.com/pvln/PVLNWB/split_display.adp?fedfid=15655651&vname=pvlrnotallissues&fn=15655651&jd=pvlr_8_1535&split=0.

[61] Sonaecom, Answers to Questionnaire with a View to Take Stock of the Data Retention Directive, *available at* https://www.vorratsdatenspeicherung.de/images/DR-consult/csp_sonaecom.pdf.

[62] Sebastien Schweda, *Austria: Council of Ministers Agrees on Data Retention*, 2011, *available at* http://merlin.obs.coe.int/iris/2011/4/article9.en.html.

[63] Thomas Breinstrup, *Dommere siger nej til EU-overvågning* [Judges Say No to EU Monitoring], BUSINESS.DK, Mar. 2, 2010, http://www.business.dk/tech-mobil/dommere-siger-nej-til-eu-overvaagning.

Even where government can subsidize the costs of compliance with data retention mandates, there are some burdens that government reimbursement cannot alleviate: data retention requires that both financial and technical resources are diverted away from innovation and invested instead in the creation and maintenance of complex data storage systems. As the US ISP Association wrote in Congressional testimony: while "[c]ost recovery could address some of the potential negative impact of a data retention requirement…in many ways reimbursement falls short of compensating industry for the opportunity costs of having their experts diverted away from focus on innovating the next generation of Internet-based services."[64]

Countries that extend data retention mandates beyond ISPs to a broader array of access-point providers impose similar capital and operating costs on those entities, thereby burdening many small retail businesses and other establishments (such a coffee shops, Internet cafes, and libraries) that seek to attract customers by offering free wireless Internet access. Smaller businesses can be particularly hard hit, as they are typically less able to comply with a mandate than are large national chain shops; schools and employers can also be impacted by such a law.

Similarly, requiring OSPs that provide services such as e-mail, chat, blogging, and social networking websites to retain "source data" tracking the origins of all user communications can create a devastating burden. As one example, in mid-2009 users on Facebook posted one billion chat messages *per day,*[65] all of which, were the U.S. to pass such a retention mandate, would have to be tracked in a database; a mandate on Facebook alone would likely require that company to add more than *one trillion* entries to a mandated retention database every year.[66] The cost of creating and maintaining such a database would be hard for any company to handle, but a retained data mandate would be especially hard on small and innovative websites seeking to compete with the larger players. Most successful sites on the Internet began as small start-ups and a retention mandate on online companies would chill the development of new sites and services. A data retention mandate can thereby damage the global competitiveness of a country's domestic technology companies.[67]

---

[64] US ISPA Testimony. *See also* EU Joint Industry Statement ("Furthermore, operational costs are increased by dedicated staff. Often the most qualified engineers, who are being asked to deal with the requests for information from LEAs or to give evidence in Court, are the most expensive and demanded resources.")

[65] *See* Chris Piro, *Chat reaches 1 billion messages sent per day*, FACEBOOK, June 15, 2009, at http://www.facebook.com/note.php?note_id= 91351698919&id=9445547199.

[66] Facebook's user base has more than doubled since the one billion chat message mark was hit in 2009, and thus it is likely that the chat message count has at least doubled. On top of that, Facebook reports that users post more than a billion other pieces of content to the site each day. *See* "Statistics," at http://www.facebook.com/press/info.php?statistics. Collectively, this equals in the neighborhood of 1.1 trillion separate user communications that Facebook would have to track in a data retention database each year.

[67] "The Data Retention Directive has a significant impact on industry and affects European competitiveness." EU Joint Industry Statement at 1.

IV. Alternatives to Data Retention

A. Numerous countries have rejected data retention

Many countries have explicitly rejected legislative data retention mandates. The reasons these countries have given for rejecting data retention laws vary, but they have generally reflected concerns about the impact of data retention laws on fundamental human rights and on business.

Argentina: In 2004, Argentina enacted a data retention law that would have required ISPs to store traffic data for ten years.[68] The law faced considerable opposition from ISPs while it was in development and in February 2005, an Internet industry trade association brought an action against the law.[69] Domestic press brought attention to the law in April 2005,[70] and by the end of the month, facing heated opposition to the law from both the public and ISPs,[71] the president suspended enforcement.[72] In 2007, Argentina's Supreme Court ruled that Articles 1 and 2 of the data retention law and a related rule were unconstitutional under Articles 18 and 19 of the national constitution, which protects the right to privacy.[73]

Canada: In 2002, the Canadian Department of Justice began consulting with industry and the public about ways to empower law enforcement to issue data preservation orders; a bill to accomplish this end was introduced in 2005.[74] Unlike a blanket data retention mandate, these data preservation orders would only require prospective retention of data about specific individuals whom law enforcement is investigating.[75] In suggesting data preservation rather than data retention,[76] the government in essence acknowledged that it was yielding to citizen, civil society, and industry concern[77] about a data retention mandate. Even with that concession, the law was not ultimately passed. In 2009 and again in 2010, the Canadian Department of Justice

[68] Law No. 25,873, Feb. 6, 2004. *See also* PRIVACY INTERNATIONAL, PHR 2006, ARGENTINA— PRIVACY PROFILE (Dec. 18, 2007), https://www.privacyinternational.org/article/phr2006-argentine-republic.

[69] *See* Press Release and Attached Documentation, CABASE, Comunicada de Prensa – 13 de Abril, 2005 [Press Release of April 13, 2005] (Apr. 13, 2005), *available at* http://www.cabase.org.ar/paginas.php?id=7.

[70] "Invasión a la Privacidad," Página 12, April 10, 2004.

[71] Press Release and Attached Documentation, CABASE, Comunicada de Prensa – 13 de Abril, 2005 [Press Release of April 13, 2005] (Apr. 13, 2005), *available at* http://www.cabase.org.ar/paginas.php?id=7.

[72] Decree No. 357/2005, Apr. 22, 2005, *available at* http://infoleg.mecon.gov.ar/infolegInternet/anexos/105000-109999/105679/norma.htm.

[73] "Halabi v. Poder Ejecutivo Nacional," Supreme Court of Argentina, June 26, 2007.

[74] Canadian Internet Policy and Public Interest Clinic, Law Access: Police Surveillance, June 2, 2007, http://www.cippic.ca/en/projects-cases/lawful-access/#LA11.

[75] *Id.*

[76] Canadian Department of Justice, Summary of Submissions to the Lawful Access Consultation, Lawful Access FAQ (2005), http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html.

[77] Canadian Department of Justice, Summary of Submissions to the Lawful Access Consultation, available at http://www.justice.gc.ca/eng/cons/la-al/index.html.

called for (but did not receive) new investigative tools – including data preservation authority – both times specifically rejecting data retention because of its overbroad impact.[78]

South Africa: In 2002, South Africa passed an expansive law entitled the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA). RICA established that providers of Internet services, an ambiguously defined class that might include access-point providers and online service providers as well as ISPs,[79] would be required to store traffic, IP allocation, and location data for a 3-5 year period.[80] The law directs the Minister of Communications to issue implementing regulations.[81] However, when the regulations were published in 2006, they spelled out data retention for so-called "fixed-line operators"[82] and "mobile-cellular operators."[83] In response to a concerted lobbying effort by the nation's ISPs,[84] the regulations omitted any mention of the retention requirements for many Internet-related telecommunications service providers.[85]

---

[78] Canadian Department of Justice, Backgrounder: Investigative Powers for the 21st Century Act (Nov. 2010) *http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32567.html*; Canadian Department of Justice, Backgrounder: Investigative Powers for the 21st Century (IP21C) Act (Jun. 2009), *http://justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32388.html.*

[79] *See e.g., Service Providers and the RIC Act*, The eFiles (Harty Rushmere, South Africa), Nov. 2007, at 1, www.harty.co.za/ServeFile.cfm?FileID=80 ("It is important to note that 'electronic communications service provider' is defined to include entities termed 'Internet service providers,' which, unlike the layman's understanding of the term, is defined extremely broadly to include any entity which provides access to, or any other service related to, the Internet"); LANCE MICHALSON & MIKE SILBER, MICHALSONS, HIGH LEVEL SUMMARY OF RICA (2005), http://www.irmsa.org.za/library/iforest/Michalsons%20Infosheet%20-%20RICA%20Summary.pdf; *ISPs Run Risk of R 5 Million RICA Fine*, MYBROADBAND.CO.ZA, Jul. 3, 2009, http://mybroadband.co.za/news/Telecoms/8643.html ("According to one industry expert this is an incredibly broad definition, and could easily include a company providing Internet access to its staff, a school providing Internet access to students or web hosting company."); Press Release, Internet Service Providers' Association, ISPA Adds Voice to Interception Objections (Jul. 3, 2006), *available at* http://www.ispa.org.za/press-release/ispa-adds-voice-to-interception-objections; Bill with Additional Amendments for Inclusion in the Judicial Matters Amendment Act, 2010, *available at* http://www.justice.gov.za/legislation/bills/2010_judmatamendBill_addamend20100311.pdf (Bill to clarify the definition of "Internet service provider" in RICA).

[80] RICA—South Africa, Section 30(2)(a)(iii).

[81] RICA—South Africa, Section 30(2)-(3).

[82] Directives in Respect of Different Categories of Telecommunications Service Providers made in terms of The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002) – Notice 1325 of 2005 [hereinafter RICA Notice 1325], Schedule A: Directive for Fixed Line Operators in Terms of Section 30(7)(a) read with Section 30(2) of The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002), Part 5: Storage Period for Communication-Related Information, 17. Period for which communication-related information must be stored (2005), *available at* http://www.acts.co.za/ric_act/ric_act.htm.

[83] RICA Notice 1325 ,Schedule B : Directive for Mobile Cellular Operators in terms of Section 30(7)(a) read with Section 30(2) of the Regulation of Interception of Communications Information Act, 2002 (Act No. 70 of 2002), Part 3: Routing, Provision and Storing of Real-Time Communication-Related Information, 9. Routing and content of additional real-time communication-related information during active intercept or in respect of future information (2005), *available at* http://www.acts.co.za/ric_act/ric_act.htm.

[84] Mike Silber, Internet Service Providers' Association Advisory 14: ISPA Member Update on RICA (Oct. 13, 2006), http://old.ispa.org.za/regcom/advisories/advisory14.shtml.

[85]RICA Notice 1325, Schedule C: Directive for Internet Service Providers in terms of Section 30(7)(a) read with Section 30(2) of the Regulation of Interception of Communications Information Act, 2002 (Act No. 70 of 2002), Part 1: Introductory Provisions, 3. Statement of General Duties (2005), *available at* http://www.acts.co.za/ric_act/ric_act.htm.

Sweden: In March 2011, the Swedish government announced that it would postpone transposition of the EU DRD for at least a year. Had it passed, the Swedish implementation would have required entities to store traffic data for the minimum period of time permitted by the Directive, six months. However, enough members of Parliament (1/6 of the membership) opposed the law on the grounds that it limited basic rights and freedoms that they were able to force a delay in its transposition.[86] In refusing to implement the Directive, Sweden risked a court case and a fine of 17-68 million Euros. The three political parties responsible for the delay are calling for the Swedish government to negotiate the Directive at the EU level.[87]

US: The US has enacted a data preservation requirement but to date (September 2011) has not adopted a data retention mandate. (However, the leading ISPs do voluntarily keep records of IP address allocations.[88]) The US data preservation law authorizes any governmental entity, without any judicial permission, to require ISPs and online service providers to retain data – including IP address and customer identifying information – for 90 days, with an additional 90 days available on request. In the child pornography context, data preservation is automatic in cases where service providers report possible child pornography to the National Center for Missing and Exploited Children (NCMEC).[89] Whenever a provider sends a child pornography report to NCMEC, the provider must automatically preserve the data to give law enforcement enough time to open an investigation and, if appropriate, obtain lawful process to demand the preserved data.[90] In July 2011, data retention legislation advanced in the Judiciary Committee of the US House of Representatives.[91] As of writing, this bill has not been passed into law.

B. Data Preservation

Government agencies do have legitimate interests in accessing communications information in order to fight crime. Data preservation is a common alternative to data retention that can help law enforcement while minimizing the impact on fundamental human rights. Data preservation permits law enforcement to require service providers to retain data for a period of time, such as 90 or 180 days, while investigators prepare the paperwork or seek judicial authorization to demand disclosure of the data.[92]

---

[86] Mikael Ricknäs, *Swedish Parliament Delays Approval of Data Retention Law, IDG NEWS,* Mar. 17, 2011, http://www.pcworld.com/businesscenter/article/222426/swedish_parliament_delays_approval_of_data_retention_law.html.

[87] Jan Libbenga*, Sweden postpones EU data retention directive, faces court, fines,* THE REGISTER, Mar. 18, 2011, http://www.theregister.co.uk/2011/03/18/sweden_postpones_eu_data_retention_directive/.

[88] AMERICAN CIVIL LIBERTIES UNION, CELL PHONE LOCATION TRACKING REQUEST RESPONSE – CELL PHONE COMPANY DATA RETENTION CHART (Sept. 2010), http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

[89] *See* United States of America, 18 U.S.C. § 2258A(h).

[90] Written Testimony of John B. Morris, Jr (Center for Democracy & Technology) before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism and Homeland Security on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes," Jan. 25, 2011, http://judiciary.house.gov/hearings/pdf/Morris01252011.pdf.

[91] For more information, *see* United States House of Representatives: Committee on the Judiciary, Mark Up Information for HR 1981, http://judiciary.house.gov/hearings/mark_07272011.html (last visited Oct. 7, 2011).

[92] In addition to the US, Japan also has a data preservation (rather than data retention) law. The law was enacted in June 2011 as part of a broader cybercrime law. *See* http://www.moj.go.jp/keiji1/keiji12_00025.html (Japanese).

From a privacy and civil liberties perspective, the benefits of the data preservation approach are enormous. Under a data preservation regime, only data about the tiny fraction of individuals who might fall under criminal suspicion is subject to a data preservation requirement. Data preservation is also far preferable from a business perspective. Under a data preservation regime, service providers can focus their attention and scarce resources on competition and innovation, rather than building tracking databases full of customer information.

V. Responding to data retention proposals

Faced with a proposed data retention mandate, advocates should work with businesses whose ability to offer innovative services will be impacted by a data retention mandate and policymakers invested in protecting human rights.

When evaluating a proposed data retention law, businesses, advocates, and policymakers should first seek to answer the following basic questions about the law:

- What types of entities will be required to retain data?
- What types of data will be retained?
- What will be the length of the retention period?
- Will the data retention mandate have extraterritorial applications?
- Who will bear the financial burden of the capital and operating costs related to data retention?
- How is government access to retained data restricted?
- How are commercial uses of retained data restricted?
- Is retained data securely held and securely transferred to law enforcement?

Where the answers to these questions include long retention periods, requirements that implicate a broad swath of companies and types of data, or weak protections for retained data, advocates and policymakers should work to limit the breadth of the retention requirements and to strengthen protections against abuse of retained data.

In addition, advocates, industry members, and policymakers should consider the potential impact of data retention on the domestic economy and on human rights:

- Does data retention respect the human rights guaranteed by the country's constitution?
- What impact will data retention mandates have on the cost of providing Internet service via ISPs or access points like coffee shops, Internet cafes, libraries, and businesses? What impact will data retention have on individuals' abilities to access the Internet?
- Will data retention mandates reduce competition amongst ISPs?
- Will government reimbursements – if they exist – sufficiently cover the opportunity costs of prioritizing data retention?
- How will the increased volume of data impact service providers' ability to respond to law enforcement inquiries in a timely fashion?
- Will data retention mandates affect the viability of online service providers or force them to relocate to other countries?

Finally, advocates, industry members, and policymakers should investigate whether data preservation is a plausible alternative to data retention.

After all, while data retention is one tool for addressing new law enforcement challenges, it is a tool that comes with a very high cost and that is ultimately disproportionate to the goals it seeks

to advance. Alternative, less privacy-burdensome programs are likely able to accomplish the government's goals just as effectively and perhaps more effectively.

###

About the Center for Democracy & Technology // www.cdt.org

The Center for Democracy & Technology is a non-profit public interest organization working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

For further information, please contact:

Cynthia Wong
Director, Project on Global Internet Freedom
+1 202-637-9800
cynthia@cdt.org

Erica Newland
Policy Analyst
+1 202-637-9800
erica@cdt.org

APPENDIX: CASE STUDIES

I. Data Retention in Europe

In 2006, the European Union issued Directive 2006/24/EC, known as the Data Retention Directive or the DRD. The Directive directs member countries to implement in law a requirement that all telecommunications providers retain all subscribers' traffic data, location data, and IP allocations for a period of six months to two years. Under the Directive, the data may only be requested by law enforcement in investigations of "serious crime" (although there is no shared definition of "serious crime"), must be stored subject to appropriate security measures, and may not be used for purposes other than those permitted by the Directive or the EU's privacy laws. The DRD, read in combination with these laws, prohibits retention of content data and URLs.[93]

Although some EU countries already had retention requirements in place before the Directive was issued,[94] the Directive has been poorly received by civil society, national legislatures, and the courts. Civil society groups have formed specifically to fight the Directive and its national transpositions.[95] The European Data Protection Supervisor Peter Hustinx has said that the DRD is "the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects."[96]

In 2009, the Romanian Constitutional Court invalidated the country's transposition of the DRD, holding that the national implementation fundamentally violated the right to respect for private life and correspondence guaranteed by the European Convention on Human Rights and the Romanian Constitution. The Court's decision emphasized that the law "overturn[ed] the

---

[93] Art. 5 of *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT [hereinafter EU DRD]; Article 29 Data Protection Working Party, Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, (July 13, 2010) at 6, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf [hereinafter WP29].

[94] *See e.g.,* PRIVACY INTERNATIONAL, POLAND— PRIVACY PROFILE (Jan. 23, 2011), https://www.privacyinternational.org/article/poland-privacy-profile#surv; PRIVACY INTERNATIONAL, PHR 2006 — ITALIAN REPUBLIC (Dec. 18, 2007), https://www.privacyinternational.org/article/phr2006-italian-republic; PRIVACY INTERNATIONAL, GREECE— PRIVACY PROFILE (Jan. 22, 2011), https://www.privacyinternational.org/article/greece-privacy-profile.

[95] *See e.g.,* EDRI.org, Campaign, Telecommunication Data Retention http://www.edri.org/campaigns/dataretention (last visited Oct. 5, 2011); AK Vorrat, Stoppt die Vorratsdatenspeicherung!, http://www.vorratsdatenspeicherung.de/static/portal_de.html (last visited Oct. 5, 2011).

[96] Peter Hustinx, Remarks at the conference Taking on the Data Retention Directive: The Moment of Truth for the Data Retention Directive (Dec. 3, 2010), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

presumption of innocence," created an "intrusion into…private life [that is] excessive," and violated the principle of proportionality.[97]

In 2010, the German Constitutional Court held that the country's transposition of the Directive, by failing to adhere to the principle of proportionality, violated the right to private life and correspondence guaranteed in the German Constitution. The Court required that all data held under the law be immediately deleted and ordered that all collection be suspended.[98]

In February 2011, the Cyprus Supreme Court declared the country's transposition of the Directive unconstitutional.[99] In March, 2011, the Czech Constitutional Court overturned the Czech Republic's transposition of the Directive, finding that the law conflicted with the right to informational self-determination and the principle of proportionality.[100] The Court also held that the Czech law does not place appropriate limits on how police can use retained data. The Court wrote that "measures as to the request and use of retained data are being overused by authorities engaged in criminal proceedings for purposes related to investigation of common, i.e. less serious crimes."[101] In Poland, members of Parliament have asked the Polish Constitutional Tribunal to evaluate the constitutionality of the country's transposition of the Directive.[102] A case concerning data retention arising in Ireland is pending before the European Court of Justice, which may consider whether data retention is compatible with the European Convention of Human Rights.[103]

Although each EU member state was supposed to transpose the Directive by 2009,[104] many countries delayed implementation. Austria initially explained that it would not transpose the DRD because the Directive itself violates fundamental rights guaranteed by the European Convention on Human Rights and the European Charter of Fundamental Rights.[105] However, after the

---

[97] Decision no.1258, Romanian Constitutional Court, Oct. 8, 2009. Published in the Romanian Official Monitor, no. 789, Nov. 23, 2009. English translation (unofficial): http://www.legiinternet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.

[98] Bundesverfassungsgericht [BVerfG][Federal Constitutional Court] Mar. 2, 2010, 1 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 256/08 (F.R.G.), *available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html*; Judy Dempsey, *German Court Orders Stored Telecom Data Deleted,* N.Y.TIMES, Mar. 2, 2010, *available at* http://www.nytimes.com/2010/03/03/world/europe/03iht-data.html; *See also* Eddan Katz, *The Beginning of the End of Data Retention*, EFF DEEPLINKS BLOG, Mar. 10, 2010, https://www.eff.org/deeplinks/2010/03/beginning-end-data-retention.

[99] *See also Data Retention Law Provisions Declared Unlawful in Cyprus,* EDRI-GRAM No. 9.3, Feb. 9, 2011, http://www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus.

[100] Press Release, Constitutional Court of the Czech Republic, Ústavní Soud Zrušil Část Zákona o Elektronických Komunikacích [Constitutional Court Struck Down Part of the Electronic Communications Act] [in Czech, with link to the decision] (Mar. 31, 2011) *available at* http://www.concourt.cz/clanek/5068.

[101] *Czech Constitutional Court Rejects Data Retention Law,* EDRI.org, Mar. 31, 2011, http://www.edri.org/czech-decision-data-retention.

[102] Katarzyna Syska, Polish Rules on Data Retention and Population Surveillance May Possibly be Subject to a Ruling of the Constitutional Tribunal, MEDIALAWS BLOG, Mar. 6, 2011, http://www.medialaws.eu/polish-rules-on-data-retention-and-population-surveillance-may-possibly-be-subject-to-a-ruling-of-the-constitutional-tribunal/.

[103] *Irish Court Allows Data Retention Law to be Challenged in ECJ,* EDRI-GRAM No. 8.10, May 19, 2010, http://www.edri.org/edrigram/number8.10/data-retention-ireland-ecj.

[104] EU DRD Art.15, Section 3.

[105] Press Release, Bundesministerium für Verkehr, Innovation und Technologie [Federal Ministry for Transport, Innovation, and Technology], Bures-Appell an Fekter und Bandio-Ortner: Vorratsdatenspeicherung im EU-Rat neu diskutieren (Jan. 1, 2010), http://www.bmvit.gv.at/presse/aktuell/nvm/2010/0129OTS0146.html.

European Court of Justice found Austria guilty of violating its EU treaty obligations, the country's parliament agreed to implement the Directive.[106] Sweden announced in March 2011 that it would risk a fine of 17-68 million Euros rather than transpose politically unpopular data retention requirements.[107] In Norway, concerns about the privacy rights implicated by the Directive created long delays in its transposition; only in March 2011 was a political agreement reached, allowing Parliament to finally begin transposing the Directive.[108] Even the UK, which played a key role in crafting the Directive, expressed reticence about retention of digital records. The coalition government formed in May 2010 pledged to "end the storage of internet and email records without good reason.""[109]

However, not all of Europe has dismissed the DRD as overbroad. For example, in March 2011, France issued a new decree pursuant to its Law for Confidence in the Numerical Economy (LCEN) that placed draconian requirements on online service providers. Under the decree, hosting companies must preserve for one year after the deletion of an account a long list of traffic data, a list that includes the password associated with the account.[110] One month after the decree was issued, a group of twenty online service providers, including Google and Facebook, lodged a complaint against the decree with the State Council, France's highest judicial body.[111]

In its 2010 review of the DRD, the European Commission's Article 29 Working Party concluded that the Directive had opened a Pandora's box of security risks and privacy violations. The review found that ISPs were illegally and regularly retaining content information such as website URLs and headers of e-mail messages and that data was not being deleted after the expiration of the mandated retention period.[112] The Working Party additionally voiced concern about generally weak or non-existent limitations on law enforcement access to retained data, pointing out that the Directive contains no shared definition of serious crime and no specific guidance to ensure that authorities only used information for purposes laid down in the directive. The Working Party also concluded that a shorter maximum retention period would better protect human rights and further harmonize practices across the continent.[113] However, this recommendation was not echoed in the Commission's April 2011 evaluation of the Directive.[114]

---

[106] Sebastien Schweda, *Austria: Council of Ministers Agrees on Data Retention*, 2011, *available at* http://merlin.obs.coe.int/iris/2011/4/article9.en.html.

[107] Jan Libbenga, *Sweden postpones EU data retention directive, faces court, fines,* THE REGISTER, Mar. 18, 2011, http://www.theregister.co.uk/2011/03/18/sweden_postpones_eu_data_retention_directive/.

[108] Rolleiv, Solholm, *Agreement on Controversial Data Retention Directive,* THE NORWAY POST, Mar, 29, 2011, http://www.norwaypost.no/political/agreement-on-controversial-data-retention-directive-24967.html.

[109] HM Government, *The Coalition: our programme for government* (Cabinet Office: London 2010)(UK) 11.

[110] Decree No. 2011-219 of Feb. 25, 2011, Journal Officiel de la Republique Francaise [J.O.][Official Gazette of France], Mar. 1, 2011, p. 3643, *available at* http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000023646013&dateTexte=&oldAction=rechJO&categorieLien=id. *See also French Decree Establishes What Data Must be Retained by Hosting Providers,* EDRI-GRAM No. 9.5, Mar. 9, 2011, http://www.edri.org/edrigram/number9.5/data-retention-hosting-france.

[111] *Google, Facebook Take France to Court over Privacy,* AFP, Apr. 11, 2011, *available at* http://www.google.com/hostednews/afp/article/ALeqM5gcIROpaIgngw8P1fO7BXywMIhe5Q?docId=CNG.897aaf456d2691082257863ec5125653.311.

[112] WP29.

[113] WP29.

[114] *Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC),* COM (2011) 225 final (Apr. 18, 2011), http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

II. Data Retention in Thailand

In July 2007, Thailand enacted the Computer Crimes Act (CCA), which includes a requirement that all "service providers" retain "computer traffic data" for 90 days.[115] The law instructs the Ministry of Information and Communication Technology to issue implementing regulations and compliance guidance.

While the text of the CCA suggests that the retention requirement applies only to telecommunication and email providers, the regulations issued by the Ministry one month after the law was enacted offered an expansive interpretation of the terms "service providers" and "computer traffic data." The term "service provider" is defined to include telecommunication and broadcast carriers (including ISPs) as well as all access-point providers and online service providers.[116] The definition of the term "computer traffic data" has also been expanded to include location data, traffic data, IP address allocations, and URLs. Online service providers must additionally keep records of user IDs, email addresses, and any messages posted by users.[117] The CCA also applies extraterritorially to Thai citizens located outside of Thailand and to non-citizens whose activities impact a Thai person or the Thai government. These regulations have led others to call the Act "one of the most expansive mandatory data retention requirements in the entire world,"[118] despite its relatively short retention period.

The extraterritorial applications of the law, if enforced, stand to have a severe impact on the Thai economy. In theory, the CCA applies to all online service providers that offer their blogs, email services, or other services to users located in Thailand.[119] In August 2010, the Thai Ministry of Information and Communication technology opened an investigation around whether the data storage practices of BlackBerry-maker Research in Motion violated the law. The ministry dropped the investigation shortly thereafter.[120]

---

[115] Computer Crime Act BE 2550 (2007), Vol 124, Section 27 Kor, *Government Gazette,* 18 June 2007 (Th.), unofficial translation available at http://www.prachatai.com/english/node/117.

[116] Belgian-Luxembourg/Thai Chamber of Commerce, Netherlands—Thai Chamber of Commerce, & Irish-Thai Chamber of Commerce, Computer Crime Seminar (Oct. 29, 2008), *available at* http://www.beluthai.org/cms/images/stories/news_items/ComputerCrimeAct_notes-Paul.pdf; Notification issued by the Ministry of Information and Communication Technology re: Procedures in Maintaining Computer Traffic Data by Service Providers, Aug. 21, 2007 (Thailand).

[117] Tim Bass, Slideshow from Presentation to the AMCHAM ICT Committee & Internet Service Providers on the Computer Crime Act B.E. 2550(2007) & Ministry of ICT Notification, 2008, http://www.slideshare.net/TimBassACIS/computer-crime-act-be-2550-2007-ministry-of-ict-notification-presentation. Also cite the original (Notification issued by the Ministry of Information and Communication Technology re: Procedures in Maintaining Computer Traffic Data by Service Providers, Aug. 21, 2007 (Thailand).

[118] John Fotiadis and Yingyong Karnchanapyap, *Computer Crimes Update,* Tilleke & Gibbons/Thailand: IP Developments), September 2008, http://www.tillekeandgibbins.com/publications/pdf/IP_bulletin_sep08.pdf.

[119] *Id; See also* MICT on International Warpath, POLITICAL PRISONERS IN THAILAND BLOG, Feb 21, 2011, http://thaipoliticalprisoners.wordpress.com/2011/02/21/mict-on-the-international-warpath/ (Translating a booklet that explains the CCA: “Does everyone know that the bill regulating computer crimes is subject to penalize the wrongdoer outside the Kingdom of Thailand as well? If there is anyone who starts a website outside the country to distribute information disgracing the monarchy, destroying the security of the justice system or generating fear among Thai people, the wrongdoer will be persecuted by law and receive penalties inside the Kingdom of Thailand”).

[120] Saksith Saiyasombut, Thailand Joins the Anti-BlackBerry Ban(d)wagon (UPDATE: Or does it?), ASIANCORRESPONDENT.COM, Aug. 20, 2010, http://asiancorrespondent.com/39212/thailand-joins-the-anti-blackberry-bandwagon-update-or-does-it/.

III. Data Retention in India

India has long required that ISPs sign the "License Agreement for Provision of Internet Services" prior to commencing operation.[121] The agreement mandates that ISPs retain "all commercial records with regard to the communications exchanged on the network." These records "shall be archived for at least one year for scrutiny by the Licensor for security reasons and may be destroyed thereafter unless directed otherwise by the licensor."[122] The term "commercial records" is not defined in the agreement. However, the document does specify that ISPs are responsible for maintaining "a log of all users connected and the service they are using (mail, telnet, http etc.)." ISPs must also "log every outward login or telnet through their computers…Type of logins, where the identity of the logged-in user is not known, should not be permitted."[123] Industry insiders report that in practice, information is archived for periods ranging from three months to a year.[124] The license does not include any privacy protections related to further use of retained data[125] and India has no general privacy law.[126]

In 2009, India enacted amendments to its 2008 Information Technology Act (ITA).[127] These amendments put into law for the first time a data retention mandate.[128] Two different sections of the ITA establish data retention requirements. The first of these sections, Section 67C ("Preservation and Retention of Information by Intermediaries") requires that intermediaries – a category broadly defined to include ISPs, online services providers, and at least some access-point providers[129] – retain a to-be-specified amount of information for a to-be-specified period of time. The law directs the government to issue rules establishing the information to be retained and the retention period.[130] As of October 2011, these rules had not yet been promulgated.[131]

---

[121] Department of Telecommunications, Ministry of Communications & IT, Government of India, "License Agreement for Provision of Internet Services"(hereinafter "License Agreement – India")(Jan. 2010) *http://www.dot.gov.in/pmrts/LICENSE%20AGREEMENT%20For%20PROVISION%20OF%20commercialPUBLIC%20MOBILE%20RADIO%20TRUNKING%20SERVICE.pdf.*

[122] License Agreement – India, Section 34.23.

[123] License Agreement – India, Section 34.8.

[124] Sunil Abraham, Does the Government want to enter our homes?, THE CENTRE FOR INFORMATION & SOCIETY BLOG, Aug. 13, 2010, http://www.cis-india.org/advocacy/igov/blog/government-enter-homes.

[125] License Agreement – India. Also *see Id.*

[126] The Indian Centre for Internet & Society asks "Do these ISPs and telecom operators then delete, anonymise or obfuscate this data? Or do they retain it for posterity for market research? In the absence of a privacy law — the Indian citizen can only make intelligent guesses." Sunil Abraham, Does the Government want to enter our homes?, THE CENTRE FOR INFORMATION & SOCIETY BLOG, Aug. 13, 2010, http://www.cis-india.org/advocacy/igov/blog/government-enter-homes.

[127] The Information Technology (Amendment) Act, 2008 (No. 10 of 2009)(In.), *available at* http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf [hereinafter ITA—India].

[128] The original ITA, enacted in 2000, did not include the retention requirements. These were added in 2008. The 2000 version of the Act can be found at http://www.mit.gov.in/content/view-it-act-2000.

[129] ITA—India, Section 2(w). *See also ITA 2000 Amendments … Impact on IT Companies*, NAAVI.ORG, Jan. 27, 2009, http://www.naavi.org/cl_editorial_09/edit_jan27_itaa_analysis_11_ites.htm.

[130] ITA—India, Section 67(C).

[131] Department of Information Technology, Ministry of Communications & Information Technology, Government of India, *Notification under IT (Amendment) http://www.mit.gov.in/content/notifications* (Last visited Oct. 6, 2011).

The second relevant section of the ITA is Section 79(2), under which intermediaries are protected from liability for third party content provided that they "observe due diligence while discharging" notice-and-takedown requirements of the law. The law directs the government to promulgate rules that set standards for due diligence.[132]

On April 11, 2011 the Indian Department of Information Technology, Ministry of Communications and Information Technology published two sets of rules that establish the government's standard for what constitutes "due diligence" by an intermediary pursuant to Section 79(2) of the ITA.[133] The rules require cybercafés, in their capacity as intermediaries, to store for one year the traffic data and "history of websites accessed" for each user.[134] Users must be identified by their government-issued ID number and photograph.[135] The rules that establish due diligence requirements for other types of intermediaries are silent on the subject of data retention, likely reflecting the fact that these rules will be issued separately, in accordance with Section 67C.

[132] ITA—India, Section 79 (2008).

[133] Information Technology (Intermediaries guidelines) Rules, 2011. (In.), *available at* http://www.mit.gov.in/sites/upload_files/dit/files/due_dilligance4intermediary07_02_11.pdf.

[134] Section 5(3) of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 (In.), *available at* http://www.mit.gov.in/sites/upload_files/dit/files/guidelines4cybercafe0702_11.pdf.

[135] Section 5(1) of Information Technology (Guidelines for Cyber Cafe) Rules, 2011 (In.), *available at* http://www.mit.gov.in/sites/upload_files/dit/files/guidelines4cybercafe0702_11.pdf.