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

INTRODUCTION TO DATA RETENTION MANDATES

September 2012

This memo introduces the concept of data retention, describes the common attributes of data retention laws, and discusses the risks to human rights, broadband deployment, economic growth and law enforcement effectiveness that such laws create.

I. What is data retention?

The telephone network (both fixed and wireless) and Internet services generate huge amounts of transactional data that reveals the activities and associations of users. Increasingly, law enforcement officers around the world seek such information from service providers for use in criminal and national security investigations. In order to ensure the ready availability of such data, some governments have imposed or have considered imposing mandates requiring communications companies to retain certain data – data that these companies would not otherwise keep – about all of their users. Under these mandates (imposed by law or regulation or through licensing conditions), data must be collected and stored in such a manner that it is linked to users' names or other identification information. Government officials may then demand access to this data, pursuant to the laws of their respective countries, for use in investigations.[1]

As a tool for addressing law enforcement challenges, data retention comes with a very high cost and is ultimately disproportionate to the goals it seeks to advance. Less privacy-burdensome alternatives are likely to accomplish governments' legitimate goals just as effectively and perhaps more effectively.

II. Data Retention: The Basics

Data retention laws vary with respect to the types of companies, data, and services that they cover.

Types of companies covered: Most of the data retention laws that have been adopted thus far focus on telephone companies (both fixed line and wireless) and Internet service providers (ISPs), including cable companies and mobile providers. Some data retention laws go further and apply to any entity that offers Internet access, such as Internet cafes, coffee shops, libraries, or companies that provide their employees with access to the Internet at work.

---

[1] For more details about data retention mandates, *see* Center for Democracy & Technology "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development" (Oct. 2011), http://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf.

Some data retention laws place retention obligations on a third category of entities: online service providers (OSPs), such as web-hosting services, email services, video-hosting sites, social networks, and blogging platforms.

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

Data retention laws can require telephone companies to retain the originating and destination numbers of all phones calls. They may require wireless companies to maintain data showing the location of users based on what cell tower they are near.

The laws may also require ISPs to retain logs of the IP (Internet Protocol) addresses they assign to their users. In general, every time a device is connected to the Internet, it is assigned an IP address by its ISP or mobile carrier. 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 unique and is associated with a particular communication as it is transmitted through the Internet. In some cases, the servers at the destination of the communication – for example, the servers that host the website the user is visiting or the instant messaging service she is using – log the source IP address and time stamp associated with each communication that they receive. Government agents may obtain the source IP addresses and timestamps from these destination servers. With this information in hand, the government can often identify the ISP or mobile carrier that provided the sender's IP address, because publicly available records show which ISPs and mobile carriers use which blocks of IP addresses. The government can then ask the originating ISP or carrier to determine which customer was assigned the particular source IP address during the relevant time period.

Increasingly, however, due to changes in technology, as a communication is in transit, the IP address of origination may be replaced by a different IP address (a "public facing" IP address), one that is not unique to a specific end-user device. This practice can result in the assignment of a new, public facing IP address as often as once per minute per device. Where this is done, ISPs and mobile carriers would have to retain an extraordinary amount of data about each of these swaps in order to allow the identification of users.[2]

Policymakers proposing data retention laws, however, are often unaware of these complexities.

Under some data retention laws, ISPs, access-point providers, and online service providers that provide communications services such as webmail or VOIP are required to record the traffic data of individual communications. Traffic data may include addressing or routing information, information relating to the identity of participants 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 destination URL information and/or precise geolocation data, such as latitude and longitude information generated by a mobile phone.

Data retention laws generally do not require companies to retain the content of communications. The EU's Data Retention Directive, for example, prohibits retention of content data.[3]

---

[2] For more details, *see* Center for Democracy & Technology "Compliance with a Data Retention Mandate: Costs Will Skyrocket with Trends in Internet Addressing" (Feb. 2012), https://www.cdt.org/files/pdfs/data%20retention%20memo%202-1-12.pdf.

[3] Art. 1, Section 2 and Recital 13 of *Directive 2006/24/EC, available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT.

Length of retention period: The "retention period" is the length of time for which companies are required to store user data. It might range from 30 days to two years.

Financial burden: Data retention laws 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. 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.

Restrictions on access to retained data: Important questions concern the conditions under which government officials can gain access to retained data. Some data retention laws may allow access only in investigations of specified crimes. A related question is the source of authority for access (is judicial approval necessary?) and the level of suspicion or justification, if any, that must be met. In many countries, standards for access to data are weak, and in national security cases they may be especially weak. It is also important to consider whether laws adequately limit the use of retained data by service providers themselves.

III. Risks Posed by Data Retention Mandates

Even where law enforcement access to retained data is appropriately limited, data retention laws create risk of significant harms.

These risks are caused, in part, by the astonishing volume of data stored and often transmitted to law enforcement under retention mandates. For example, in 2009, Danish ISPs reported that, in order to comply with the country's retention law, they collected an average of 82,000 data records per Dane.[4]

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.[5]

A. Data retention laws violate fundamental human rights

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. These rights are reflected both in the provisions of numerous international and regional agreements and in decisions rendered by human rights tribunals.[6]

These human rights concerns are not theoretical. At least one study has shown that data

---

[4] 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.

[5] *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.

[6] *See e.g.,* The Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (Art. 6.2), Universal Declaration of Human Rights (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.

retention in Europe has significantly diminished citizens' willingness to discuss and obtain information about mental health issues online.[7] In Poland, intelligence agencies used data stored under the country's data retention laws to expose information about journalists' sources.[8]

Human rights institutions have found that data retention mandates 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."[9] In 2008, the National Human Rights Commission of Korea, an independent governmental body charged with analyzing laws from a human rights perspective, 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…[10]

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. 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 have held that their nation's data retention mandates were unconstitutional because they violated the principle of proportionality. [11]

Data retention laws also create new types of privacy risks. Retained data, especially where stored by entities – such as coffee shops and schools – that have not traditionally kept such customer data, is vulnerable to hackers, accidental disclosure, and other unauthorized access, thereby aggravating the identity theft problem. There is also a risk that retained data may be put to other legal, but privacy-invasive uses. For example, service providers, once forced to invest in building databases of customer information, may decide to repurpose that data for other uses, such as behavioral advertising.

---

[7] *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.

[8] 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).

[9] Article 29 Data Protection Working Party, Report 01/2010 on the Second Joint Enforcement Action (July 13, 2010) at 6, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf.

[10] 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.

[11] Bundesverfassungsgericht [BVerfG][Federal Constitutional Court] Mar. 2, 2010, *available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html*; Nález Ústavního soudu (Czech Republic Constitutional Court) cj. 24 / 2010, *available at* http://www.concourt.cz/clanek/GetFile?id=5075; Decision no.1258, Romanian Constitutional Court, Oct. 8, 2009. English translation (unofficial), http://www.legiinternet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.

B. 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. A major reason is cost. By definition, a data retention law requires companies to store data that they have no business reason to retain. 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.[12]

Many parts of the world receive broadband services from small ISPs, which often serve communities or regions that larger ISPs do not reach. Small ISPs typically operate with tiny profit margins and would be unable to absorb the many costs of data retention. The National Telecommunications Cooperative Association (NTCA), a US-based trade association for small and rural telecommunications cooperatives,[13] estimated that complying with the data retention mandate found in legislation proposed by the U.S. House of Representatives in 2011 would create capital costs for a typical rural broadband provider that would amount to between 5 and 7.5% of its annual revenue and would likely run some of these ISPs out of business,[14] thereby reducing broadband deployment in the United States.

Even where government can subsidize the costs of compliance with data retention mandates, data retention diverts technical and personnel resources away from innovation and devotes them instead in the creation and maintenance of complex data storage systems.[15]

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. Small, local businesses, and even schools and employers, can be particularly hard hit, as they may be poorly equipped to comply with a mandate. 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. Most successful sites on the Internet began as small start-ups that could not conceivably retain the required data; a retention mandate on

---

[12] *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.

[13] These cooperatives are often customer owned and supported by the US government's Universal Service Fund.

[14] National Telecommunications Cooperative Association (NTCA), "Dynamic IP Address Assignment and Tracking," 2011. The costs will vary for each ISP as each network is different. The quoted cost range is for two different models for compliance that NTCA considered. In developing its cost estimates, NTCA made various assumptions about rural telecommunication companies and their existing infrastructure, the need to fully upgrade new infrastructure, the cost of equipment, and the cost to send a technician to each subscriber location (if required under the compliance approach). These assumptions should not be assumed to be accurate for every network. According to NTCA, the loans required to finance these capital investments would very often be provided by the USDA Rural Utilities Service. However, due to the stringent loan review processes that are in place to ensure the appropriate use of taxpayer dollars, the loan approval process can take up to two years.

[15] US ISPA Testimony. *See also* 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.

online companies would therefore chill the development of new sites and services. A data retention mandate can thereby damage the global competitiveness of a country's domestic technology and discourage investment by foreign technology companies.

C. Data retention laws may hinder law enforcement efforts

Because it increases the ratio of low-value data to high-value data, data retention mandates can be quite ineffective, hindering law enforcement's ability to access the information it needs in a timely manner. Large-scale data storage increases the likelihood of system crashes; the greater the volume of stored data, the less reliable its integrity and the longer the delays when ISPs respond to law enforcement requests. This can create a perverse result in emergency situations: law enforcement may find it has slower access to needed data, because ISPs must sort through mountains of data to find what is needed. The data most desired in emergencies is often recent data that would likely have been retained and more easily accessible absent a retention mandate.[16]

IV. An Effective Alternative to Data Retention: Data Preservation

Data preservation is an alternative to data retention that can help law enforcement while minimizing the impact on human rights. Under a data preservation regime, a law enforcement officer can demand that an Internet company begin storing – "preserving" – data relevant to a *specified* investigation or proceeding. Typically, the company is required to continue preserving this data for a period of time, such as 90 days. Both the US and Japan have data preservation, and not data retention, laws.[17]

The US has a more complex data preservation regime specifically for the child pornography context. Under US law, whenever ISPs become aware of possible child pornography on their networks, they must submit a report to the US child abuse hotline, run by the National Center for Missing and Exploited Children (NCMEC).[18] When it makes such a report, the provider must *automatically* preserve the data associated with the suspected child abuse images so that, if law enforcement officials open an investigation, they can obtain lawful process to demand the preserved data.

From a privacy and civil liberties perspective, the benefits of the data preservation approach are enormous. Under a data preservation regime, companies retain only data about the tiny fraction of individuals who might fall under criminal suspicion. Data preservation is also far preferable from a business perspective because it allows service providers to focus their attention and scarce resources on competition and innovation, rather than building and maintaining databases full of customer information, the vast majority of which will never be used.

For further information, contact Jim Dempsey, Vice President for Public Policy, jdempsey@cdt.org

---

[16] 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).

[17] *See* Title 18 United States Code § 2258A(h). Japan's law was enacted in June 2011. *See* http://www.moj.go.jp/keiji1/keiji12_00025.html (Japanese).

[18] *See* Title 18 United States Code § 2258A.