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: ANALYZING A DRAFT LAW

APRIL 2012

This document introduces the concept of a "data retention" law and offers a hypothetical data retention law of the type that might be introduced in any country around the world. The reader is asked to imagine that this law is being proposed by "Country Y," a country with a robust Internet economy that is the home to many successful online service providers. A set of questions is then used to guide the reader through an evaluation of the law.

I. Introduction

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. 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.

II. Hypothetical law proposed in imaginary Country Y

Imagine that Country Y is a large country that is home to many successful Internet services. For example, one of the world's most popular social networking services was started in Country Y and is headquartered there. Lawmakers in Country Y are debating whether to pass a data retention law that would apply to all Internet service providers (ISPs), Internet access-point providers (such as Internet cafes and coffee shops), and online service providers (such as those offering email and social networking services) located in Country Y.

The law proposed by lawmakers in Country Y reads:

Section 1:

All **Internet Service Providers**, **Internet Access-Point Providers**, and **Online Service Providers** with offices in the country must retain all **Location Information** and **Traffic Data** generated by users of their services. This data must be retained in a form such that it is linked to an identified individual. This data must be retained for a period of 18 months and must be deleted after 18 months. This data must be retained in a form such that it can be provided to law enforcement within 24 hours of a legal request. The data must be provided to law enforcement within 24 hours of a legal request.

Section 2:

All **Internet Service Providers**, **Internet Access-Point Providers**, and **Online Service Providers** must pay for all costs associated with compliance with this law.

Section 3:

A legal request from law enforcement is a request for the **Location Information** or **Traffic Data** generated by a single individual. This request must be signed by a judge. A judge may only sign such a request if the request is for information generated by a criminal suspect or a person whom law enforcement has shown is likely to have interacted with the criminal suspect during the past 18 months.

Section 4 (Definitions):

Internet Service Provider means a mass-market service, sold on a standardized basis to such entities as residential customers and businesses, that provides access to the Internet.

Internet Access-Point Provider means an entity, such as a coffee shop, library or Internet café, that provides temporary Internet access to individuals.

Online Service Provider means an entity that makes available a website, application, or piece of software that receives information through the Internet.

Location Information means information relating to the location of an individual user.

Traffic Data means information relating to the identities of users involved in an exchange of information over the Internet, email headers and subject lines, the date, time, duration, and type of the communication, any URLs visited, and information about the type of network and equipment involved in this exchange of information.

III. Evaluating the proposed law

Imagine you have been asked to evaluate the proposed law. Think about how you would answer the following questions:

1. What is the law intended to achieve and is the goal legitimate?
2. Who is directly targeted for new legal obligations or rights under this law?
3. Who else will likely be benefited or harmed by the law and how?
4. Is the law consistent with International human rights norms and with other regional or international commitments?

5. Does the proposed law work with the Internet's essential attributes or does it seek to change them? How?[1]

6. Is this a concern that government should address or is it best dealt with through other means?

7. If government intervention is appropriate, are there other policy approaches to achieve this goal that are more protective of rights and the Internet's essential attributes?

8. What precedents are available from other countries to suggest other less intrusive approaches?

9. As an advocate, would you support or oppose the proposed law? Why or why not?

10. If you oppose the law, who else do you think would oppose the law? What types of individuals and entities would you try to bring into the coalition you would organize to fight the law? Why would you choose them?

11. What will be the most effective arguments against the law?

12. Who are your key audiences and what are the best messages for those audiences?

13. If you are unlikely to defeat this data retention law, are there changes you can propose to the law that would narrow its impact on privacy? What additional safeguards would you propose?

IV. Discussion Points for reviewing the evaluation questions

1. What is the law intended to achieve and is the goal legitimate?

    a. The law is being created to provide law enforcement access to information about criminal suspects.

    b. In order to know if the law will be used for non-legitimate goals, it would be helpful to find out more information about the legal system and law enforcement powers in Country Y. Does Country Y classify as criminal certain behavior that is clearly protected by international human rights norms?

2. Who is directly targeted for new legal obligations or rights?

    a. Internet Service Providers (ISP)s, Online Service Providers (OSPs), and Internet access-point providers (cafes, etc) are all targeted for new legal obligations.

    b. Law enforcement is granted new rights.

3. Who else will likely be benefited or harmed by the policy and how?

    a. Foreign OSPs will likely benefit. This law will increase costs for companies with offices in Country Y and put companies located elsewhere in a more competitive position. (As one example, as far back as mid-2009 users on Facebook posted one

[1] The Internet is open and decentralized; is neutral and nondiscriminatory; has lower barriers to entry; offers an abundance of points of entry; is global and borderless; is user-centric and user-controlled, and is versatile. These are the essential attributes of an open Internet.

billion chat messages *per day.* Imagine having to retain data associated with each of those messages over an 18-month period!).

b. Similarly, the economies of other countries will benefit as those OSPs located in Country Y leave the country and move to other countries.

c. Broadband deployment would be harmed. This law would increase costs for ISPs and would likely force small ISPs to close. This would increase the costs of broadband and delay deployment in rural areas.

d. Many Internet access-point providers (coffee houses, Internet cafes) would probably have to stop providing Internet access. They would likely not be able to afford the huge costs associated with storing so much information.

e. Law enforcement efforts may benefit, but they may also be harmed. 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.

f. Individuals will be harmed – this type of data collection flips the principle of "innocent until proven guilty" on its head. See discussions points for Question 5.

g. In addition to the *prima facie* privacy violations created by data retention, the practice also increases the risks of damaging data breaches and identity theft. The practice additionally increases the chance that companies, already required to retain this data, will sell it to data brokers or put it to other privacy invasive uses. Here we see the intersection of concerns over privacy vis-à-vis government and vis-à-vis companies.

4. Is the law consistent with International human rights norms or with other regional or international commitments that Country Y may have?

   a. 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.

   b. At least one study has shown that data retention in Europe has significantly diminished (German) citizens' willingness to discuss and obtain information about mental health issues online.

   c. Because this law allows access to data related to anyone who might have communicated with someone suspected of a crime, the records of many non-criminals will likely be accessed.

   d. The law can hurt the functioning of a free press: In 2010, the Polish press reported that the country's weak limits on law enforcement access to retained data had enabled abuse of the country's data retention law. As part of a politically motivated plot, agents accessed mobile phone location and traffic data stored under the data retention law. In the Netherlands, data stored under the countries' data retention laws has exposed information about journalists' sources.

5. Does the proposed law work with the Internet's essential attributes or does it seek to change them? How?

a. This law would make the Internet, as experienced by all people using services with offices in Country Y (whether or not those people are citizens of Country Y), less user-centric and user-controlled.

6. Is this a concern that government should address or is it best dealt with through other means?

    a. Yes, this is a concern that government should address.

7. If government intervention is appropriate, are there other policy approaches to achieve this goal that are more protective of rights and the Internet's essential attributes?

    a. Data preservation is one option: Data preservation is a common alternative to data retention that can help law enforcement while minimizing the impact on fundamental human rights and business. 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 up to a maximum period of time, such as 90 days. These requests are known as *data preservation* requests. Both the US and Japan have data preservation, and not data retention, laws.

    b. From a privacy and civil liberties perspective, the benefits of the data preservation approach are enormous. Under a data retention mandate, data about all individuals is retained, creating high compliance costs, violating the rights of all Internet users, and making it more difficult for ISPs and law enforcement to identify the data that they actually need. Under a data preservation regime, data about only the tiny fraction of individuals who have fallen under criminal suspicion is subject to a data preservation requirement. Everyone else would continue to enjoy the same level of privacy he or she would otherwise enjoy regardless of the law enforcement investigation. 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.

    c. See answers to Question 8 below.

8. What precedents are available from other countries to suggest other less intrusive approaches?

    a. Some countries with data retention laws only require that ISPs and mobile carriers retain data (For example, this is the approach taken by the EU's Data Retention Directive). This limits the impact on Internet access-point providers and OSPs.

    b. Another approach is to only require ISPs to store IP address allocations. IP address allocations indicate which subscriber was assigned which IP address for a particular period of time. However, due to the changing technology of IP address allocations, this can also prove very expensive. See https://www.cdt.org/files/pdfs/data%20retention%20memo%202-1-12.pdf.

    c. Some laws limit data retention to only six or twelve months. Studies have shown that data from the most recent past is the most useful to law enforcement.

    d. Some countries require that the government pay for some of the costs of retention and for the costs associated with compliance with law enforcement requests. This creates a cost burden for law enforcement that helps prevent them from making an excessive number of requests.

9. As an advocate, would you support or oppose the proposed law? Why or why not?
10. If you oppose the law, who else do you think would oppose the law? What types of individuals and entities would you try to bring into the coalition you would organize to fight the law? Why would you choose them?
    a. Domestic ISPs, OSPs, and those who serve as Internet Access Points (libraries, schools, coffeehouses, Internet cafes, etc.).
    b. Free speech and privacy advocates and academics.
    c. Journalists who are concerned about this data being used to reveal their sources (as has happened in Poland and the Netherlands)
11. What will be the most effective arguments against the law?
12. Who are your key audiences and what are the best messages for those audiences?
13. If you are unlikely to defeat this data retention law, are there changes you can propose to the law that would narrow its impact on privacy? What additional safeguards would you propose?
    a. Section 1
        i. Have the law apply only to ISPs
        ii. Have the law apply only to IP address allocations, instead of Location Information and Traffic Data. IP address allocations indicate which subscriber was assigned which IP address for a particular period of time.
        iii. Have the law only require a 6 or 12-month retention period. Data has shown that the information becomes much less useful after six months.
    b. Section 2**:** Require law enforcement to cover the costs associated with complying with a legal request. This would help limit the number of excessive requests.
    c. Section 3: Require higher standards for law enforcement access to data. For example, law enforcement should not be able to view all data associated with a criminal suspect (and especially not all data associated with someone who may have interacted with a criminal suspect) but instead only that data it has shown is likely related to the criminal activity.

###

For further information, please contact:

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