

## **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 phone 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?<sup>1</sup>
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?

###

**For further information, please contact:**

Cynthia Wong  
Director, Project on Global Internet Freedom  
+1 202-637-9800

---

<sup>1</sup> 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.