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

BASIC OVERVIEW OF DATA RETENTION MANDATES – PRIVACY AND COST

September 2012

Introduction

The use of telephone and Internet services generates information useful to governments in conducting law enforcement and national security investigations. In an effort to guarantee the availability of communications data for investigations, some governments have imposed or have considered imposing legal obligations requiring communications service providers to retain for specified periods of time certain data about all of their users. Generally, under these "data retention" mandates, data about individuals' use of communications services must be collected and stored in a manner such that it is linked to a specific user's name or other identification information. Government officials may then request access to this data, pursuant to the laws of their respective countries, for use in investigations.

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, and perhaps more, effectively.

I. 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 by governments around the world focus on telephone companies (both fixed line and wireless) and Internet service providers (ISPs), including cable companies cable and mobile providers. Some data retention laws also apply to any entity that offers Internet access, such as Internet cafes and WiFi "hotspots." Some data retention laws place retention obligations on online service providers (OSPs) – companies that provide, among other things, web-hosting services, email services, platforms for user-generated content, and mobile and web applications.

Types of data covered: "Data retention" laws can require telephone companies to retain the originating and destination numbers of each phones call. 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. Under some data retention laws, ISPs, access-point providers, and OSPs that provide communications services such as webmail or VOIP are required to record the traffic data of individual users. Traffic data may include addressing or routing

information associated with each communication, information relating to the identity of 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 destination URL information. Data retention laws generally have not required covered entities to retain the content of communications.

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: The cost of data retention mandates includes data storage centers, systems retrieving data 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.

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.

II. Problems Created by Data Retention Laws

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

- Data retention, by creating records that link highly detailed descriptions of users' communications 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 broadband deployment and innovation in the ICT industry, particularly by making it hard for new companies to launch.
- Data retention, because it increases the ratio of low-value data to high-value data, may ultimately be ineffective as it can hinder law enforcement's ability to access the information it needs in a timely manner, especially in emergency situations.

III. Alternatives to Data Retention: Data Preservation

"Data preservation" is an alternative to data retention and a more proportionate measure that can help government investigators while minimizing the impact on fundamental human rights and business. Under a data preservation regime, a law enforcement officer can demand that a communications provider *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, while government agents obtain the necessary authority to compel disclosure. Under a data preservation system, only data about the tiny fraction of individuals who might fall under criminal suspicion is stored. Both the US and Japan have data preservation, and not data retention, laws.

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