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: Changes in Internet Addressing Technology Affect Cost, Effectiveness, and Proportionality

September 2012

Some governments have imposed or are considering imposing on telecommunications service providers requirements to maintain certain data about their customers' communications. This paper focuses on such data retention mandates as they apply to data about Internet usage. It explains how changes in Internet addressing technology are rendering data retention mandates for Internet IP addresses increasingly more expensive and less effective and therefore less proportionate as responses to the interests of law enforcement.

I. Introduction

Over the past decade, some governments have imposed or have considered imposing data retention mandates on telecommunications service providers and other communications companies, requiring that they store certain data about all of their users' communications, even when it is not needed for business purposes. Under these mandates, this 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, for use in investigations.[1] Such data retention laws impact individuals who have no connection whatsoever to criminal activity.

Data retention laws vary considerably with respect to the companies, types of data, and services that they cover. However, many of the data retention laws that have been adopted require Internet service providers (ISPs) to retain records of which IP addresses they have allocated to which users. (By "ISP" we mean traditional cable or DSL Internet access providers as well as mobile carriers that provide Internet access.) Some data retention laws also require other entities that offer Internet access – including Internet cafes, coffee shops, libraries, or companies providing Internet access to their employees at work – to retain records of IP addresses allocations.[2]

In this paper, we focus on how changes in Internet addressing technology are rendering laws that require the retention of IP address allocations more costly and less effective and therefore less proportionate than they were even five years ago.

---

[1] This paper is adapted from a CDT memo, "Compliance with a Data Retention Mandate – Costs Will Skyrocket with Trends in Internet Addressing" (Feb. 1, 2012) https://www.cdt.org/files/pdfs/data%20retention%20memo%202-1-12.pdf.

[2] Some data retention laws also require traditional telephone companies, both wireline and wireless, to record the originating and destination number of all calls and require wireless providers to record the physical location of callers. These types of retention obligations are out of scope for this paper. *See* Erica Newland and Cynthia Wong, "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development," Center for Democracy & Technology, Oct. 2011 (hereinafter "CDT Data Retention Paper"), http://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf.

This paper analyzes the costs these IP-address-focused data retention mandates would impose on ISPs as well as on businesses, such as Internet cafes, that offer Internet access to their customers. It specifically focuses on developments in Internet addressing practices that will make the costs of data retention much larger than previously understood. It also explains why, as a result of those same trends in address allocation, IP address data may no longer reliably identify individual end-user devices, thus reducing the effectiveness of data retention mandates.[3]

First, we describe a major development in Internet addressing: ISPs are increasingly sharing Internet addresses among multiple customers, which means that IP addresses no longer uniquely identify the computers or other devices of individual Internet users. We then explain why this trend in IP address sharing means that, increasingly, if ISPs or other businesses are to retain the types of IP-address allocation data in which governments are interested, they must collect vastly larger quantities of data at considerably greater cost than may have been projected even several years ago. We explain why, at the same time that the data is becoming more voluminous, it is also becoming less effective for identifying individual users. We next discuss how compliance costs can especially harm small ISPs, such as those that provide Internet access for rural or otherwise underserved communities or regions. Finally, this memo examines the implications of IP address sharing and data retention mandates for Internet cafés, hotels, other businesses, and NGOs, most if not all of which use address sharing when they provide Internet access for visitors or employees. These entities, where covered by a data retention mandate, may be forced to either assume the huge costs of data retention or forgo providing Internet connectivity altogether.

II. Changes underway in IP address sharing render compliance with data retention mandates extraordinarily expensive, but less effective

The high capital and operating costs associated with data retention mandates have long been identified as drawbacks of data retention laws.[4] However, recent changes in technology are making data retention mandates far costlier to effectively implement than they were even a few years ago.

First, some technical background: In the simplest configuration of Internet access, each device is assigned a unique Internet Protocol address when it is connected to the Internet. That "IP address" is associated with each communication originating from that device and generally stays with the communication as it is transmitted over the Internet. In some cases, the servers

[3] For more about the privacy implications of data retention mandates, *see* CDT Data Retention Paper, note 2 above.

[4] Capital costs associated with data retention compliance include the costs of designing new collection and storage systems, purchasing collection and storage equipment, integrating new and existing systems, and developing systems to identify and deliver requested data to the government in a timely manner. Key operating costs associated with compliance include the costs of operating and maintaining interfaces for accessing the data in a timely manner, data security, compliance implementation staff, law enforcement liaison staff, staff training, system maintenance, and continuing system integration efforts. *See* 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 (hereinafter "EU Joint Industry Statement"), https://www.vorratsdatenspeicherung.de/images/DRconsult/csp_joint_statement.pdf.

at the destination of the communication – for example, the servers that host the website the user is visiting or the instant messaging service being used – log the source IP address associated with each communication that they receive as well as the time of each communication. In many jurisdictions, government agents may obtain the source IP addresses and timestamps either from these destination servers or by other means (such as by seizing and searching the computer of the recipient of the communication). With this information in hand, the government can often identify the ISP that provided the sender's IP address, because publicly available records show which ISPs use which blocks of IP addresses. The government can then ask the originating ISP to determine which customer was assigned the particular source IP address during the relevant time period.[5] Many data retention mandates require ISPs, and sometimes other entities, to retain logs of the IP addresses they assign so that they can connect the IP address obtained by law enforcement at the end point of a communication to a particular customer at the communication's starting point.

Increasingly, however, ISPs are not using the simple configuration of Internet access described above. Instead, in a growing number of circumstances, the IP address that passes over the Internet is no longer unique to a single end-user device. As we explain below, this change makes it complex and extraordinarily expensive for some ISPs to collect and retain the data necessary to retrospectively connect the source IP address as recorded at the end of a communication to the individual customer who originated the communication.

These changes are being driven by a critical shortage of traditional IP addresses, known as IPv4 addresses. In response to this shortage, key Internet stakeholders have embarked on a potentially decades-long transition to a new addressing protocol, known as IPv6. In the meantime, major Internet access providers around the globe are adopting a very complex system of assigning IP addresses that helps conserve IPv4 addresses.

This technology, known as Network Address Translation (NAT), allows multiple Internet users to share the same IP address. Until recently, NAT was primarily used at a relatively small scale – for example, to have all of the devices within a single household or Internet café share one address. However, because the pool of available IPv4 addresses is near exhaustion and in many countries the transition to IPv6 has only just begun, many ISPs have started, or are planning, to use NAT on a much larger scale.[6] As a result, in some cases, a single IP address may be shared among thousands of customers. Furthermore, because devices that are only capable of understanding one version of IP or the other need to communicate with each other during the transition phase, newer flavors of NAT have been developed to translate between IPv4 and IPv6.[7]

NAT usage, whether on a small or large scale, greatly increases the amount of data that must be stored in order to connect particular Internet activity to a specific customer. Below, we

[5] This presumes, of course, that ISPs, a category of providers that includes mobile carriers, know the identities of their customers. Where SIM cards for mobile devices are purchased without registration, mobile carriers may not have this information anyway.

[6] Use of NAT by ISPs is often referred to as Carrier-Grade NAT, or CGN.

[7] This is a crucial detail, as machines that are IPv4 compatible and machines that are IPv6 compatible cannot easily communicate with each other. Consequently, ISPs must deploy transition technologies, such as NAT, to enable IPv4-capable devices and IPv6-capable devices to communicate with each other, and the use of such transition technologies will be necessary for the foreseeable future.

explain in more detail why NAT so drastically raises the costs of compliance with data retention mandates.

A. Many IP addresses no longer uniquely identify users or end-user devices

Whenever an Internet-connected device communicates on the public Internet, it is identified by a number called a public IP address, which is typically provided by the ISP that connects that device to the Internet. Just as a street address sometimes identifies one unique individual, a public IP address sometimes identifies one unique Internet-connected device. However, just as a street address can be shared by multiple members of a family or even a large number of families and individuals, such as all those who live in the same apartment building, NAT allows a single public IP address to be shared by an entire household, all computers in an organization, or thousands of unrelated customers.

The way this works is that the ISP sets up a NAT router serving multiple users. Every device behind the router is assigned a private IP address, one that is not seen on the public Internet.[8] When one of these devices initiates a communication, the communication contains the source's private IP address and a number between 0 and 65,535 that is known as a port number.[9]

When the router behind which the device sits receives the source's private IP address and port number, it records these and then associates them with two new numbers: a public IP address that is possibly being used by many other devices sitting behind the same router and a port number that is not being used by any other device sitting behind the router. The ISP uses what is known as a translation table (hence the name "Network Address Translation") to convert between the private IP address/port number combination and the public one and thereby to ensure that the devices that share the same public IP address receive only the data intended for their respective devices.

Moreover, especially in the context of mobile Internet access, the IP address/port number combination for a particular device can change very frequently. Mobile devices can obtain a new IP address/port number combination as frequently as once every minute and possibly even more frequently.[10]

B. NAT complicates compliance with data retention mandates

Even for ISPs whose networks use an IP address allocation scheme that does not involve NAT, compliance with a data retention mandate can be quite burdensome. IP addresses within these networks may change on a daily or weekly basis and the high costs of retaining logs of these changes for six, twelve, or eighteen months can be quite burdensome.

---

[8] This system allows ISPs and mobile carriers to use just one of their assigned public IP addresses to serve multiple customers, thus stretching the limited supply of IPv4 addresses assigned to the access providers.

[9] The port number is typically associated with the specific application or process initiating a communication, but the Internet protocol provides for so many port numbers (65,536 of them) that most of them are never used to identify an application. To facilitate IP address sharing, they have been re-purposed as device identifiers.

[10] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that Phone? Geolocating IP Addresses on 3G Networks," The Proceedings of the 2009 Internet Measurement Conference (Chicago, Illinois: Nov. 2009), *available at* http://research.microsoft.com/en-us/um/people/maheshba/papers/ephemera-imc09.pdf.

For carriers and ISPs that deploy NAT, the cost and complexity of compliance with a data retention mandate can be especially high. As mentioned above, new port assignments can occur as often as once every minute.[11] Depending on the type of NAT used, to successfully maintain an association between a user and her IP address, many ISPs may have to add new data to their logs each time a new port assignment occurs. This data includes a timestamp, outgoing port number, public and private IP addresses, and a link to the customer's identifying information. For a small or medium size ISP, this may amount to a data storage requirement on the order of terabytes of data per day,[12] an enormous quantity of data to retain for six months or even years. (Imagine re-issuing a copy of a telephone directory as often as once a minute but still having to maintain every old copy for months or years.) Of course, this data is not useful for law enforcement unless ISPs also maintain the capability to sift through it, creating additional, monumental technical burdens.

As the IPv4 address shortage becomes increasingly severe and the transition to IPv6 progresses, NAT will see even larger-scale deployment. Given the complexities posed by NAT, ensuring end-user identity will increasingly require extensive and expensive recordkeeping by a wide range of entities. Purely in terms of burdens on innovation, broadband deployment, and economic growth (not to mention privacy), this new reality dramatically reduces the proportionality of data retention as a response to the legitimate needs of law enforcement.

C. NAT adds to the already high costs of data retention

Many of the data retention laws in effect around the world were written before ISPs began adopting NAT on a large scale. As such, some of these laws are unclear about what compliance means for ISPs that deploy NAT: do these laws require ISPs simply to maintain the same records they did before deploying NAT, therefore rendering the retention mandates wholly ineffective? Or do they require ISPs to retain sufficient data to successfully connect users' Internet activities to their identities, thereby creating extraordinarily burdensome costs?

When the US House of Representatives considered a data retention bill in 2011 (the bill was later withdrawn), the US ISP Association estimated that compliance with the proposed measure would cost members $500 million over 5 years while other industry representatives offered estimates of $1.6 billion.[13] One small American ISP with under 5 million subscribers told CDT that under the proposed bill, it could face operating costs of $50 million per year, not including initial capital expenses incurred for the purchase of new equipment and the development of new systems for storing and accessing data. Moreover, in the words of the US ISP Association, cost

---

[11] *Id.*

[12] ISPs and mobile carriers can choose between different approaches for allocating ports. Under a system known as dynamic port allocation, ports are assigned on an as-available basis. This is the most efficient system for ISPs and carriers to use, but it creates the unwieldy logs described. Under a system known as bulk port allocation, a specified range of ports is allotted to each customer; the customer's public communications will always be associated with one of the ports in this range, so logs don't need to be updated every time a port assignment changes. Under bulk port allocation, however, applications can malfunction for those customers who are not allotted enough ports to meet their needs. As the number of Internet-connected IPv4 devices grows, the number of ports allocated to each customer will decrease, increasing the likelihood of application malfunction under bulk port allocation. *See* S. Pareault et al, "Common Requirements for Carrier Grade NATs (CGNs) – Revision 5," Internet Draft (Nov. 30, 2011), http://tools.ietf.org/html/draft-ietf-behave-lsn-requirements-05.

[13] US House, Committee on the Judiciary, *Protecting Children from Internet Pornographers Act of 2011,* H. Rpt. 112-281, http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt281/pdf/CRPT-112hrpt281-pt1.pdf.

estimates do not typically account for the "opportunity costs of having [ISPs' technical] experts diverted away from focus on innovating the next generation of Internet-based services."[14]

D. Address sharing reduces the effectiveness of data retention

1. Address sharing increases the complexity of determining end-user identity

Data retention mandates are premised on the assumption that an IP address is a reliable Internet identifier that can be tied to an end user. With address sharing, to make a match, it is necessary to know not only the IP address associated with a communication, but also the port number and timestamp. However, the port number information necessary to make a match in a NAT context may not be logged at the destination point. Not all destination servers currently record incoming port numbers, and for some it may be difficult or impossible to configure them to do so.

To make a match using NAT tables also requires that the clock used at the destination point to set the timestamp associated with the communication of concern be synchronized with the clock of the originating ISP. However, clocks on the Internet are not perfectly synchronized.[15] If the clocks of the destination server and the Internet access provider are off, even by a few seconds, it may not be possible to make a reliable match, potentially leading to disclosure of data on innocent persons. This can be a problem especially in the mobile context, where the IP address and port number combination for a particular device may change rapidly. By complicating the process of determining end-user identity, NAT therefore reduces the effectiveness of data retention mandates.

2. Data retention mandates may hinder law enforcement efforts – and the extraneous data created by address sharing exacerbates this problem

Finally, the difficulty for ISPs of retrieving in a timely manner the information sought by the government cannot be overstated. Large-scale data storage increases the likelihood of 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 demands from government. Because it greatly increases the amount of data that ISPs have to store in order to ensure end-user identity, the use of NAT can greatly exacerbate this problem. As the US ISP Association explained in testimony before the US Congress in January 2011, data retention may delay responses in true emergencies because of the slow speed of searching through massive volumes of data.[16] This is an especially perverse result because the data most desired in emergencies is typically recent data that, absent a data retention mandate, often would have

---

[14] 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 (hereinafter "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.").

[15] See, e.g., Paul Krzyzanowski, "Clock Synchronization" (2009) http://www.cs.rutgers.edu/~pxk/417/notes/content/08-clocks.pdf.

[16] US ISPA Testimony, note 14 above.

been retained for business reasons and – because of the lower volume of retained data – would have been more easily accessible.

E. Despite the deployment of IPv6, NAT will likely be used for decades

Some have argued that the problems posed by address sharing will evaporate when IPv6 is fully implemented because IPv6 will have enough addresses to assign one to each Internet-connected device. However, while some Internet access provider networks are already "IPv6 compatible," the full, global transition to IPv6 is likely to last many years, even decades, because there will continue to be end-user devices that are compatible only with IPv4.[17] As long as even a single application or source of content worldwide is available only via IPv4, the level of address sharing on the Internet, and the use of NAT, will continue to rise (as NAT will be needed to enable the communication between that single application or source of content and every IPv6-enabled device on the Internet).[18] In short, both the practice of sharing IP addresses and the resultant difficulty of matching destination data with source point data that arises from this sharing (see discussion immediately below) are likely to persist for many, many years.[19]

III. Data retention mandates especially burden small ISPs

Many parts of the world receive broadband services from small ISPs, without which they would remain stuck with slow dial-up services, unable to take advantage of large amounts of the content and services offered through the Internet today. Small ISPs often serve communities in which larger ISPs have not been willing to invest.

As we discussed above, the use of NAT greatly increases the many capital and operational costs of data retention – from the purchase of new equipment to the development of data

---

[17] Larry Greenemeier, "Out with the Old: As Internet Addresses Run Out, the Next-Generation Protocols Step Up," *Scientific American* (Feb. 4, 2011), http://www.scientificamerican.com/article.cfm?id=ipv4-to-ipv6-transition ("IPv4 and IPv6 will need to coexist for several decades to ensure that IPv4 devices can continue to connect to the Internet for as long as they are functioning."); Presentation by Doug Montgomery of NIST, "IPv6: Hope, Hype and (Red) Herrings" (Feb. 28, 2006), http://w3.antd.nist.gov/usgv6/ipv6-hhh-current.pdf. ("Transition period could last decades…or forever").

[18] S. Nightengale, D. Montgomery, S. Frankel, and M. Carson, "A Profile for IPv6 in the U.S. Government – Version 1.0" (Draft), Special Publication 500-267, National Institute of Standards and Technology (July 2008) http://www.antd.nist.gov/usgv6-v1-draft.pdf ("The key to a successful IPv6 transition is compatibility with the large installed base of IPv4 Hosts and Routers. Maintaining compatibility with IPv4 while deploying IPv6 will streamline the task of transitioning the Internet to IPv6. Most Nodes will need such compatibility for a long time to come, and perhaps even indefinitely.").

[19] For more on the IPv6 transition, see S. Frankel, R. Graveman, and J. Pearce, "Guidelines for the Secure Deployment of IPv6 (Draft)," Technical Report 800-119, National Institute of Standards and Technology (Dec. 2010), http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf ("because the transition to IPv6 will last a long time, implementations of IPsec on IPv4 networks are likely to continue to be used indefinitely"); Robert Cannon, "Potential Impacts on Communications from IPv4 Exhaustion & IPv6 Transition," Staff Working Paper 3, Federal Communications Commission (Dec. 2010) http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1230/DOC-303870A1.pdf.

security measures[20] and systems for retrieving data in response to government demands. These additional costs, which until now have gone largely unrecognized by lawmakers, can prove especially problematic for small ISPs, which typically operate with very small profit margins. The National Telecommunications Cooperative Association (NTCA), a US-based trade association for small and rural telecommunications cooperatives, estimated that complying with the data retention mandate found in legislation proposed (but never approved) in the US House of Representatives in 2011 would have created capital costs for a typical rural broadband provider amounting to between 5 and 7.5% of its annual revenue.[21] Such a requirement would likely run some of these ISPs out of business, thereby reducing broadband deployment in the United States and exacerbating the digital divide.[22] Similar results can be expected worldwide as data retention mandates are extended or clarified to require retention of the records created by NAT deployment.

IV. Hotels, coffee shops, airports, airplanes, buses, parks, libraries, convention centers, and a host of other access providers also use NAT

Some existing and proposed data retention mandates extend to Internet cafes, coffee shops, hotels, airports, buses, and others that offer Internet service to customers. Such entities very likely use NAT technology to distribute IP addresses within their networks. (Indeed, the use of NAT by small establishments predates its adoption at the carrier level.) All of an Internet café's customers, for example, may sit behind a NAT router with a single IP address. The same complications for data retention that NAT creates for mobile carriers and ISPs are created for the small coffee shop, the Internet café, the hotel, the bus, and the airport. We assume that there is a diversity of business arrangements by which these entities offer Internet access. In almost all these cases, however, the public-facing IP address passed through the Internet by these entities and recorded at a destination point will not be the IP address assigned to an individual end-user device. Even if a regular ISP were to keep a record of the Internet address assigned to its customer (the Internet café, hotel, employer, etc.), that customer could run a

[20] In Europe, despite data security requirements that are written into the data retention law, small ISPs have found it difficult to appropriately secure data. A recent European Commission report found the high cost of implementing security rendered these providers "unable to implement top IT security solutions protecting [retained data.]". *See* 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.

[21] The proposed legislation was known as H.R. 1981, 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.

[22] Letter from Shirley Bloomfield, CEO, National Telecommunications Cooperative Association to Rep. Lamar Smith, Chair (July 26, 2011)("Finally, the nation's 1,150 rural providers are small businesses that operate on thin margins and lack the economies of scale to absorb a large, sudden cost. The rural telecom industry bears little resemblance to the largest providers, but it is essential to connecting the entire country. NTCA members serve areas where there is no business case for service and others refuse to serve. If rural providers were to exit their markets there would typically be no provider ready to step in and provide the kind of area-wide service that the local and national economies rely on.").

NAT router providing Internet access simultaneously to dozens or even hundreds of other people.[23]

For countries that adopt new data retention laws, the popularity of NAT leads to one of two results: either small businesses like coffee shops are covered and are required to collect and maintain complex records and systems for associating the IP addresses they assign to customers with the public-facing data they pass to the Internet, *or* coffee shops, hotels and many tens of thousands of other establishments become a gaping hole in the coverage, and hence the effectiveness, of the law. In the former situation, the infrastructure needed to store months' worth of records about each customer's behavior require substantial investment in expensive equipment by the entities that are covered under the data retention mandate: the NAT routers these establishments typically use are incapable of keeping persistent logs – they simply don't have the storage capacity. Compliance with a new data retention mandate would require that these businesses discard their current equipment and purchase all new equipment at considerable cost. Indeed, whenever new data retention mandates are adopted, many small businesses – and possibly many public venues – may be unable to continue to offer Internet access.

V. Conclusion

It is widely recognized that data retention mandates have serious privacy consequences.[24] Retained information is available to the government for purposes other than those that prompted adoption of the law or introduction of proposed legislation. Stored data can be vulnerable to hackers or to inadvertent disclosure. There is evidence that data retention has a chilling effect on use of the Internet for provision of important services.[25] Data retention mandates are also likely to chill political use of the Internet and other free speech.

In this memo, however, we focused on the costs of data retention and, to some extent, on its effectiveness in light of ongoing technological changes.

In the changing Internet ecosystem, data retention has become far more complex than even we at CDT understood several years ago. The evolution of IP address assignment practices is vastly increasing the amount of data that providers have to retain in order to succesffully associate IP address information with end users. Even with modern storage capabilities, the volume will soon be so huge that the costs of data retention will skyrocket, hurting especially small carriers in regions with limited broadband deployment, as well as coffee shops, Internet café, and others that provide Internet access. This may slow or even reduce broadband deployment and divert financial and technical resources away from innovation.

---

[23] NAT can be layered on NAT. The bus or train that uses NAT may receive its service from a carrier that uses NAT.

[24] *See* CDT Data Retention Paper, note 2 above.

[25] 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 (finding that as a result of a German data retention law, "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 athttp://www.eco.de/dokumente/20080602_Forsa_VDS_Umfrage.pdf.

Meanwhile, good alternatives to data retention exist. Across the world, governments have the authority to request information relevant to a specific investigation, using methods that do not require the retention of massive amounts of information that will never be part of an investigation. In short, due to its high cost, the privacy violations it creates, its limited effectiveness, and the existence of good alternatives, data retention is an ultimately disproportionate, ineffective, and unnecessary response to law enforcement interests in user data.

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