A New Data Retention Requirement: Uniformly Opposed and Bad Public Policy

As a potential vote nears on the USA FREEDOM Act, talk about possible amendments has begun. There is one amendment in particular that poses a threat not only to the bill's passage, but to data security, privacy, and the information economy: a new data retention mandate requiring phone companies to store Call Detail Records (CDRs) for a fixed period of time, regardless of their business needs. Not only would such a requirement be harmful; it is also unnecessary for national security. The President has been clear that he does not want one, the NSA testified before the Senate Intelligence Committee that it does not need one, and the Director of National Intelligence stated in a September 2014 letter supporting the USA FREEDOM Act that a new data retention requirement is unnecessary for the Intelligence Community to meet its operational needs.

Strong Opposition From Civil Society, Security Experts, Industry, and the House of Representatives: The addition of a data retention requirement would severely undermine the unique, bipartisan, and broad-reaching coalition of supporters the USA FREEDOM Act currently enjoys. In June, July and September 2014 coalition letters on the USA FREEDOM Act, OTI cautioned that we, along with over 40 other privacy and advocacy organizations, would strongly oppose the inclusion of any new data retention requirements in surveillance reform legislation. Over 20 security experts and academics also wrote to Congress opposing such a mandate. A data retention mandate would also threaten the support of tech and telecommunications companies, like Verizon who testified before Congress that they would strongly oppose any such provision of law. In March, over 40 advocacy groups and companies, including the Reform Government Surveillance coalition, which represents some of America's largest tech companies like Google, Apple, and Facebook, signed a letter opposing the inclusion of controversial new mandates in surveillance reform legislation.

Support would not only be lost in industry and civil society. The House of Representatives overwhelmingly opposes data retention requirements, and would almost certainly refuse to pass a version of the USA FREEDOM Act that includes one. It has rejected proposals for data retention requirements several times in the past few years – most recently during its 2014 and 2015 considerations of the USA FREEDOM Act. There, the House Judiciary Committee resoundingly opposed an amendment that would have authorized the government to make individual agreements with companies for data retention. Even that amendment smacked too much of a requirement and both times failed by a vote of 24-4, with Chairman Goodlatte stating in 2014 that "record retention by the communications companies does not necessarily assuage civil liberty and privacy concerns and could expose these records to data breaches by cyber hackers. For these reasons, I cannot support this amendment."

Bad Public Policy: There is good reason for this fierce opposition to a data retention requirement. It is bad public policy. Mandatory data retention would not only threaten privacy and increase data insecurity, it would also impose unnecessary financial burdens on American technology companies, it could hinder law enforcement efforts, and it could cause regulatory problems.

For more information, please contact Robyn Greene, Policy Counsel, at greene@opentechinstitute.org.

Threat to Privacy: Requiring companies to store their customers' personal information beyond what is needed for their business practices is an inherent threat to privacy. That's why privacy and security regulators routinely counsel companies not to keep data they don't need—to minimize, rather than retain, unnecessary data. In this case, the CDR data at issue is especially sensitive, providing a detailed dossier on Americans' private communications and associations. A requirement under the USA FREEDOM Act would set a dangerous precedent—a precedent that could quickly set the stage for mandatory retention of even richer and more personal Internet data—because it would, for the first time, require that companies store Americans' private data solely so that a military intelligence agency – the NSA – could access it. This possibility was considered and explicitly rejected as a threat to privacy when the President announced the need to reform the Patriot Act Section 215 bulk collection program.

Threat to Data Security: In addition to posing a threat to privacy, a new data retention requirement would pose a serious threat to data security and could significantly increase the risk of a data breach. First, there are staggering technical difficulties to storing and securing the vast quantities of data that would be required. Second, we live in an era of data breaches. In the last two years alone, Americans' personal and financial information has been stolen from dozens of major companies like Target, Home Depot, JP Morgan, Sony, and Anthem. Passing a data retention requirement with the USA FREEDOM Act will paint a new, bigger, and brighter bullseye for hackers on the back of every company that is subject to the requirement, and thus, on each of their customers.

Threat to Business: A new data retention requirement would be extremely costly to companies. Storing exabytes of data, as would be required by ISPs, will cost many millions of dollars to set up systems for storing, securing, and searching the data, and millions of dollars more each year to maintain those systems. Additionally, Kate Dean, President of the U.S. Internet Service Providers Association, warned Congress that the opportunity cost, or the cost to innovation resulting from the diversion of business resources to the development of these storage and retrieval systems, would be incalculable. Costs to innovation make government reimbursement, which would fall squarely on taxpayers' shoulders, inadequate compensation.

Hindrance to Law Enforcement: Dean also cautioned against a new data retention requirement because it could impede law enforcement investigations. Delays in retrieving relevant data would likely result from searching large stores data since it would be more difficult to identify the specific information sought in the masses of irrelevant information. Additionally, the systems could crash altogether under the weight of the data.

Source of Regulatory Problems: Lastly, a new data retention requirement could cause significant problems in implementation because there could be conflicts between statutory and regulatory obligations, protections for users' privacy, and questions about standards for law enforcement access to records.

Ultimately, a new data retention requirement would not increase our security. Just the opposite – it would be bad for security, bad for privacy, and bad for business. The USA FREEDOM Act has a historic coalition of support. Republicans and Democrats have reached across the aisle to pass this reform. Technology companies large and small along with civil society groups from the right and left have worked together with lawmakers for nearly two years to see it pass this Congress. Now that we're nearly at the finish line, Congress should pass that bill rather than fatally undermine its chances by adding to it an unnecessary, controversial, and dangerous new data retention mandate.

For more information, please contact Robyn Greene, Policy Counsel, at greene@opentechinstitute.org.