Computer & Communications Industry Association
Tech Advocacy Since 1972

ABSTRACT

GOVERNMENT ACCESS TO DATA APRIL 2014

The current law governing surveillance does not protect people from government overreach, both in the US and abroad. Data kept with third parties is treated differently than that kept on a personal computer, and geolocation data is not protected at all. For national security investigations, there is a pervasive lack of transparency, oversight, and restriction that has led to issues of trust around the world.

The Electronic Communications Privacy Act reflects a communications reality that is nearing three decades old. To properly protect citizens' data in the 21st Century, ECPA must be reformed. The Digital Due Process Coalition's recommendations provide a blueprint for this much needed process.

The bounds of the National Security Agency's authorization, which had been secret until June of 2013, are incredibly broad and need to be narrowed. Transparency must be increased, bulk collection of data should be halted, and stricter controls on access to content should be imposed, amongst other reforms.

Background: Having balanced rules regarding government access to citizens' data is vitally important to the growth of the Internet. Consumers will only participate in online industry if they believe that the data they expose is safe, not just in the hands of the companies that they deal with, but also from overreach by the government. The statutory and constitutional rules governing this sort of access by government for criminal purposes, however, are out of date and do not reflect modern expectations of privacy. We have also learned in the past year that the rules under which national security surveillance occur are vague, interpreted in secret, and riddled with loopholes. Many have come to believe that updating these laws is of the utmost importance.

CCIA's Position: CCIA believes that the time has come to modernize our interpretation of the Fourth Amendment and amend ECPA to account for the ways technology is used today. Congress should take up ECPA reform, and follow the suggestions of the Digital Due Process Coalition, of which CCIA is a member. DDP has taken the time to analyze ECPA in light of current uses of technology, and make a list of four broad recommendations for the reform of the law. CCIA endorses these recommendations and urges Congress to adopt them as soon as possible

CCIA thinks that the USA FREEDOM Act, a bipartisan and bicameral bill, holds the most hope for reforming national security surveillance. Around the world, CCIA supports the Reform

Government Surveillance principles as a set of suggestions for all governments on the proper application of surveillance powers on the Internet.

CCIA also believes that Congress should refrain from any expansion of the Communications Assistance for Law Enforcement Act that would mandate certain technical infrastructure from Internet communications companies. Such a burdensome and unnecessary mandate would squash innovation, harm privacy, and damage cybersecurity efforts without providing an appreciable benefit to law enforcement.

Policy Considerations:

Electronic Communications Privacy Act Reform

Some of the decisions that Congress made in implementing ECPA in 1986 made sense given the technology at the time, but have aged poorly as new uses for the Internet and computers have come about. The DDP recommendations would, most pertinently, require a probable cause warrant before government could obtain private content held by third parties. The recommendations would also create the same requirement for geolocation information, which currently is not explicitly regulated and is the subject of confusion for magistrate judges and law enforcement authorities.

National Security Agency Reform

We have learned in the past year that provisions of the USA PATRIOT Act and the FISA Amendments Act have been secretly interpreted to give the government the power to peer deeply into ordinary people's lives, such as bulk collection of metadata using various authorities, including Section 215 of the USA PATRIOT Act, and warrantless collection and use of Americans' content under section 702 of the FISA Amendments Act. Finally, citizens of other countries have no protection under current law, creating widespread distrust of American companies abroad.

Communications Assistance for Law Enforcement

There are also perennial proposals to expand the Communications Assistance for Law Enforcement Act to apply to online services Expanding CALEA to cover any system that provides a platform for user communication would seriously harm innovation, privacy, and cybersecurity, and should be avoided at all costs.

Current Status: Momentum continues to build in Congress for reform of ECPA. Senator Patrick Leahy's bill – which would require law enforcement to obtain a warrant before accessing users' content – passed out of the Judiciary Committee on a voice vote last year. Its companion bill in the House, introduced by Representatives Yoder and Polis, now have nearly 200 co-sponsors. Members of DDP continue to hold meetings on Capitol Hill to develop support for the needed reforms.

Legislative action on NSA reform, on the other hand, is just getting started. Senator Leahy and Representative Sensenbrenner have introduced the USA FREEDOM Act which CCIA supports, but further movement has not yet happened. There are also proposals originating in the two

Intelligence Committees which would not adequately solve the problems with the current structure and would in some cases actually authorize further collection and use by the NSA. CCIA is opposed to these efforts. Finally, the White House itself has a number of proposals which are still vague at this point, making analysis difficult.