900 17th Street, N.W.
Suite 1100
Washington, DC 20006
Phone: 202.783.0070
Fax: 202.783.0534
Web: www.ccianet.org
Computer & Communications Industry Association

ABSTRACT

GOVERNMENT ACCESS TO DATA

April 2012

- *Current law in privacy from government intrusion does not provide the protections that people reasonably anticipate. Data kept with third parties is treated differently than that kept on a personal computer, and pervasive geolocation data is not protected at all.*
- *The Electronic Communications Privacy Act (ECPA) 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 project.*
- *A data retention mandate would burden small, independent Internet Access Providers, create privacy and cybersecurity risks, and do little to solve the problems that law enforcement is concerned about.*

Background: Having balanced rules regarding law enforcement 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 The statutory and constitutional rules governing this sort of access by government, however, are out of date and do not reflect modern expectations of privacy. The inconsistencies in the law also lead to confusion and hesitancy on the part of companies that have to comply with it, and the law enforcement officials who have to operate within it. Many have come to believe that updating the law 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 the Electronic Communications Privacy Act 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 an original 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 also believes that Congress should refrain from any expansion of the Communications Assistance for Law Enforcement Act (CALEA) that would mandate certain technical infrastructure for 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

In the late 1970s and early 1980s, it became evident that the Supreme Court's interpretation of

the Fourth Amendment did not in general extend to information handed over to a third party (this is still true today, although some appeals courts are beginning to question the approach). Noticing that individuals and companies were beginning to hand over personal computer data to others for storage or processing reasons, Congress passed the Electronic Communications Privacy Act in 1986 to lay down a set of regulations governing the legal process required by the government in order to obtain this data that a citizen had delivered to a third party.

Some of the decisions that Congress made in implementing ECPA made sense given the technology at the time, but have aged poorly as new uses for the Internet and computers have come about. As an example, the level of process that law enforcement needs to obtain access to an email depends on how old the email itself is. The DDP recommendations would, most pertinently, require a probable cause warrant before government could obtain private data held by third parties. The recommendations would also create the same requirement for geolocation information, which currently is not explicitly protected and is the subject of confusion for magistrate judges and law enforcement authorities.

CCIA is also opposed to any proposals to expand the Communications Assistance for Law Enforcement Act (CALEA) that may be attached as a part of ECPA reform. The government has for some time claimed that new telecommunications technologies should be subject to the same requirements for wiretap assistance that cover the phone system, although there has been no official proposal as of yet. 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.

Data Retention Mandates

Law enforcement relies in some cases on obtaining records from parties to be used as evidence. In particular, Internet Protocol address assignment data from Internet Access Providers can be necessary to prove that a suspect visited a particular website. Under current law, IAPs have no general duty to retain these records, but they are required to abide by requests by law enforcement to preserve certain pieces of data during the course of an investigation.

A data retention mandate, however, would be unduly burdensome, particularly on smaller IAPs. It would create privacy and cybersecurity concerns, overwhelm already understaffed FBI offices with data, and at the end of the day, remain largely ineffectual due to the use of public Internet offerings and proxy services. CCIA is therefore opposed to any generalized data retention mandates.

Current Status: Momentum is beginning to build in Congress for a reform of ECPA. Senator Patrick Leahy has introduced a bill that would require law enforcement to obtain a warrant before accessing users' content and future real time cell phone location data. Historical location data would be available with lesser process, however. Senator Ron Wyden and Representatives Jason Chaffetz and Robert Goodlatte have introduced a bill that would provide complete warrant protections for geolocation information. Members of DDP continue to hold meetings on Capitol Hill to develop support for the needed reforms.

On January 23, 2012, the Supreme Court handed down a decision in *US v. Jones* that held that a warrant is required in order for the government to collect location information via a GPS device attached to a car. While the decision rested on narrow grounds, the concurrences to the opinion

gave hope that a reexamination of the relationship between the Fourth Amendment and digital information may be forthcoming.