DIGITAL

MODERNIZING SURVEILLANCE LAWS FOR THE INTERNET AGE

ABOUT THE ISSUE
OUR PRINCIPLES
WHO WE ARE
NEWS
RESOURCES

OUR PRINCIPLES

Overarching goal and guiding principle: To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.

These principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA.

- A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.

- A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.

- A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).

- Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information

related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.

Read More: Specific Background on ECPA Reform Principles

OUR PRINCIPLES To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.

MORE ▶

MEMBERS

MORE ▶

Contact | Privacy Policy

BACKGROUND

1. The government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.

- This principle applies the safeguards that the law has traditionally provided for the privacy of our phone calls or the physical files we store in our homes to private communications, documents and other private user content stored in or transmitted through the Internet "cloud"-- private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks.
- This change was first proposed in bi-partisan legislation introduced in 1998 by Senators John Ashcroft and Patrick Leahy. It is consistent with recent appeals court decisions holding that emails and SMS text messages stored by communications providers are protected by the Fourth Amendment, and is also consistent with the latest legal scholarship on the issue.

2. The government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.

- This principle addresses the treatment of the growing quantity and quality of data based on the location of cell phones, laptops and other mobile devices, which is currently the subject of conflicting court decisions; it proposes the conclusion reached by a majority of the courts that a search warrant is required for real-time cell phone tracking, and would apply the same standard to access to stored location data.
- A warrant for mobile location information was first proposed in 1998 as part of the bipartisan Ashcroft-Leahy bill. It was approved 20 to 1 by the House Judiciary Committee in 2000.

3.Before obtaining transactional data in real time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.

- In 2001, the law governing "pen registers and trap & trace devices" - technologies used to obtain transactional data in real time about when and with whom individuals communicate over the phone - was expanded to also allow monitoring of communications made over the Internet. In particular, the data at issue includes information on who individuals email with, who individuals IM with, who individuals send text messages to, and the Internet Protocol addresses of the Internet sites individuals visit.
- This principle would update the law to reflect modern technology by establishing judicial review of surveillance requests for this data based on a factual showing of reasonable grounds to believe that the information sought is relevant to a crime being investigated.

4.Before obtaining transactional data about multiple unidentified users of communications or other online services when trying to track down a suspect, the government should first demonstrate to a court that the data is needed for its criminal investigation.

- This principle addresses the circumstance when the government uses subpoenas to get information in bulk about broad categories of telephone or Internet users, rather than seeking the records of specific individuals that are relevant to an investigation. For example, there have been reported cases of bulk requests for information about everyone that visited a particular web site on a particular day, or everyone that used the Internet to sell products in a particular jurisdiction.
- Because such bulk requests for information on classes of unidentified individuals implicate unique privacy interests, this principle applies a standard requiring a showing to the court that the bulk data is relevant to an investigation.

ResourcesTo simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.
More

More**Content on this page requires a newer version of Adobe Flash Player.**

More

Contact | Privacy Policy

DIGITAL

MODERNIZING SURVEILLANCE LAWS FOR THE INTERNET AGE

PRIVACY POLICY

Privacy Policy

DigitalDueProcess.org is committed to protecting the privacy and security of visitors to our Web Site. Outlined below is our privacy policy.

Personally Identifiable Information Collected on this Web Site

DigitalDueProcess.org may collect certain personally identifiable information from visitors to our Web site who choose to provide it through various web forms on our site. Such information will be used only for its explicitly stated purpose, and will not be otherwise disclosed or shared except as described herein. Any such information provided may be retained by DigitalDueProcess.org for a period of up to 24 months.

Privacy of our Email Lists

Visitors to our Web site may choose to subscribe to various email lists maintained by DigitalDueProcess.org. Subscribers to DigitalDueProcess.org email lists have the opportunity to remove themselves from future communications by clicking on the "unsubscribe" link at the bottom of any email message. DigitalDueProcess.org does not sell, rent, or otherwise share email addresses or other personally identifiable information with anyone outside of our coalition members and authorized agents or to the extent required by law.

Browser Information and Cookies

DigitalDueProcess.org monitors the performance of our web site through commercially available web log analysis tools. We examine aggregate information including page views, unique user sessions, and other statistics to help us assess the performance of our site. No personally identifiable information is collected as a result of this process. DigitalDueProcess.org may use cookies to enhance the user experience on our web sites. Visitors may use the site without cookies by disabling cookies on their browser;

however, doing so may render certain portions of the site inoperative.

Children's Privacy

DigitalDueProcess.org complies with the Children's Online Privacy Protection Act of 1998 (COPPA). This web site is intended for adults only, and we do not knowingly contact or collect personal information from children under 13.

General Provisions

Use of this site constitutes your consent to this policy. This policy and our privacy practices are subject to change at any time by DigitalDueProcess.org. If a change to our privacy practices is made, a corresponding change to our privacy policy will be posted here along with the date of the effect of such a change.

Last Updated March 30, 2010

OUR PRINCIPLES To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.

MORE ▶

MEMBERS Google™

MORE ▶

DIGITAL

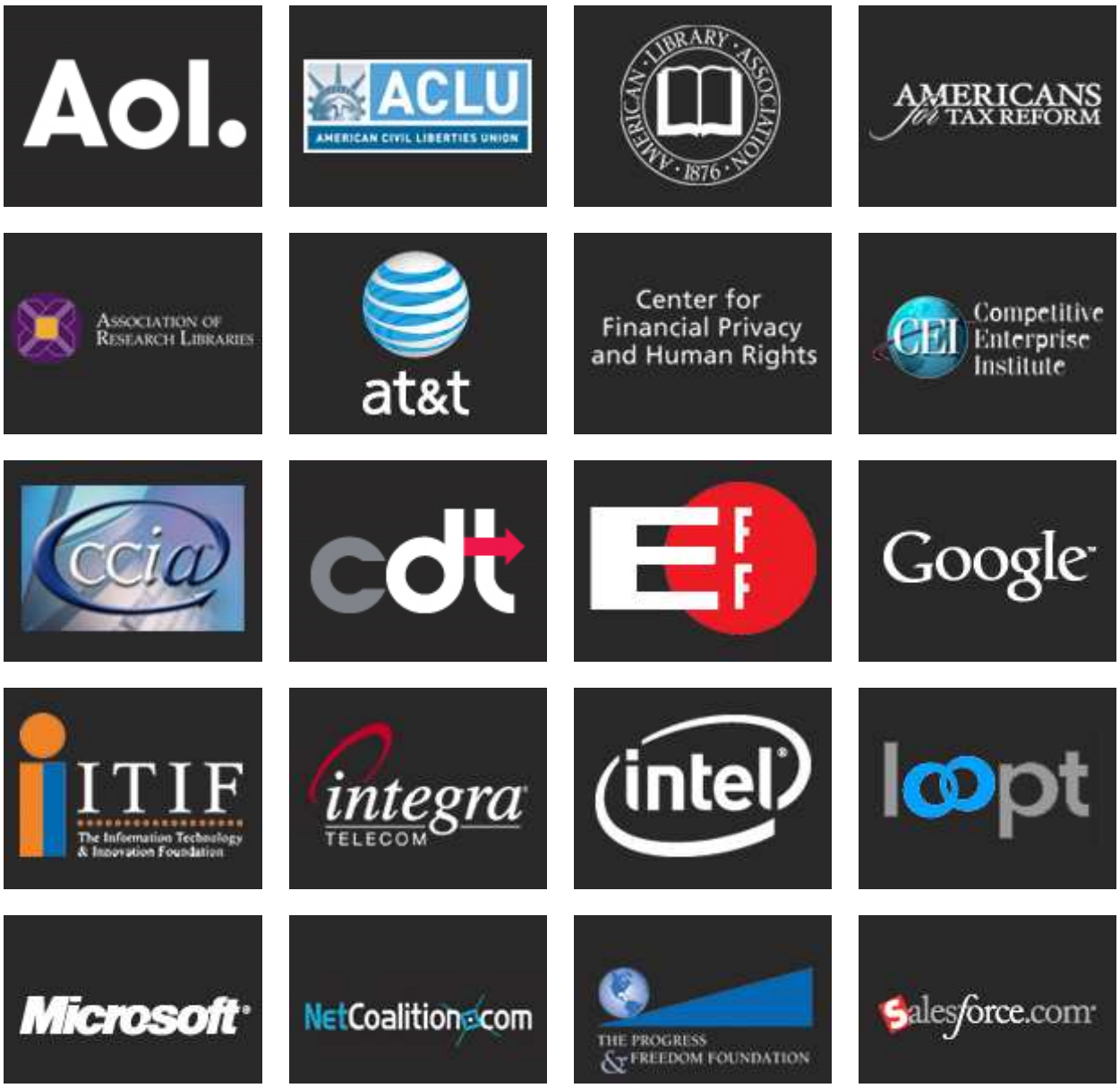
MODERNIZING SURVEILLANCE LAWS FOR THE INTERNET AGE

ABOUT THE ISSUE
OUR PRINCIPLES
WHO WE ARE
NEWS
RESOURCES

WHO WE ARE

Digital Due Process is a diverse coalition of privacy advocates, major companies and think tanks, working together.

Coalition Members Include:



Jennifer Lynch, UC Berkeley Law School
Deirdre Mulligan, UC Berkeley iSchool
Paul Ohm, Professor of Law, University of Colorado
Jennifer Urban, UC Berkeley Law School
Marc Zwillinger, Zwillinger Genetski LLP

Join our Coalition!

If your organization or company is interested in joining our coalition, please click here.

OUR PRINCIPLES

To simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public.

MORE ▶

MEMBERS

AMERICANS for TAX REFORM

MORE ▶

Contact | Privacy Policy