



# UPDATING THE LAW ON GOVERNMENT ACCESS TO USER DATA IN THE CLOUD

**James X. Dempsey**

Center for Democracy & Technology

**Richard Salgado**

Google

Session ID: LAW-402

Session Classification: General Interest

**RSACONFERENCE2012**

# Government access rules begin with the Constitution

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

- Fourth Amendment (1791)



# Notwithstanding technological change, some things have remained pretty clear:

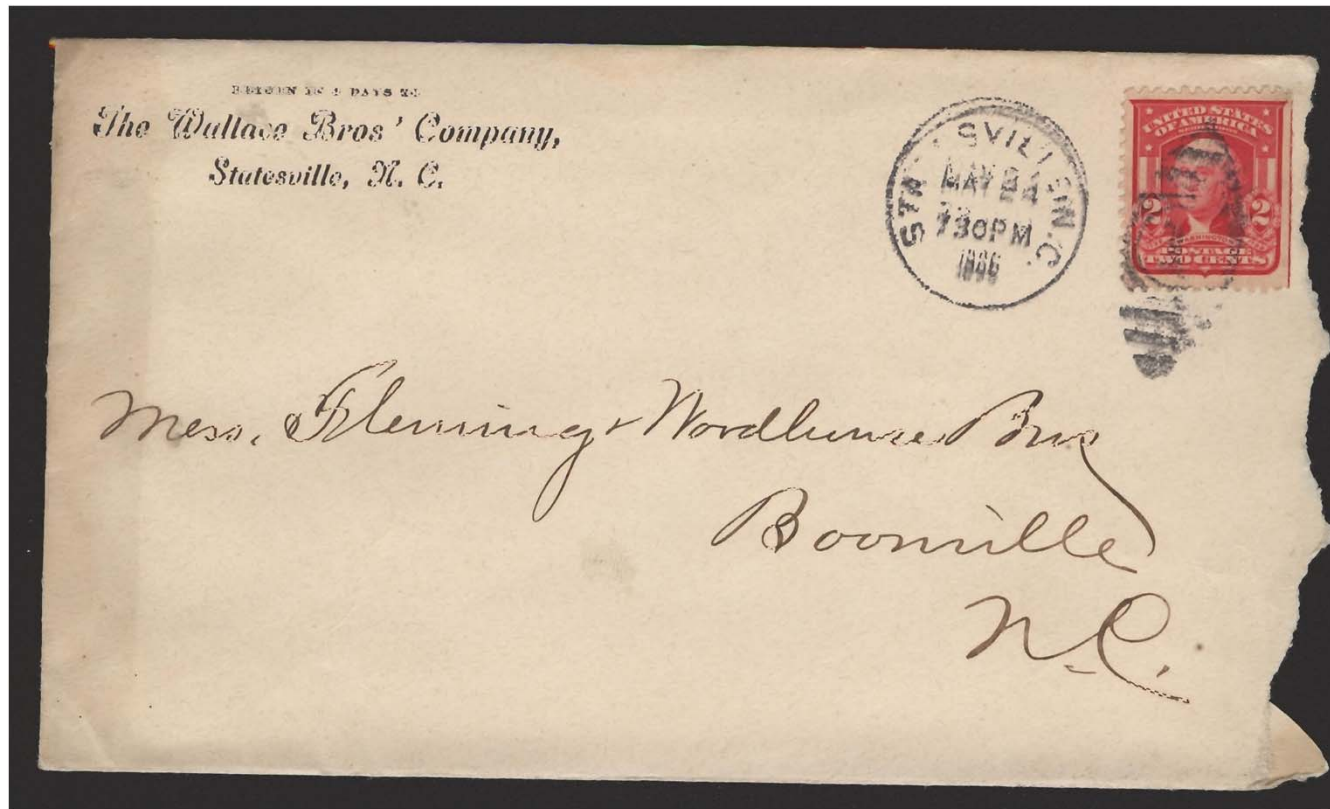
Data, regardless of technology --

- in your home or office
- in your briefcase or wallet
- on your laptop
- on any device in your possession --

is fully covered by the 4th Amendment, normally requiring a search warrant issued by a judge for government access.



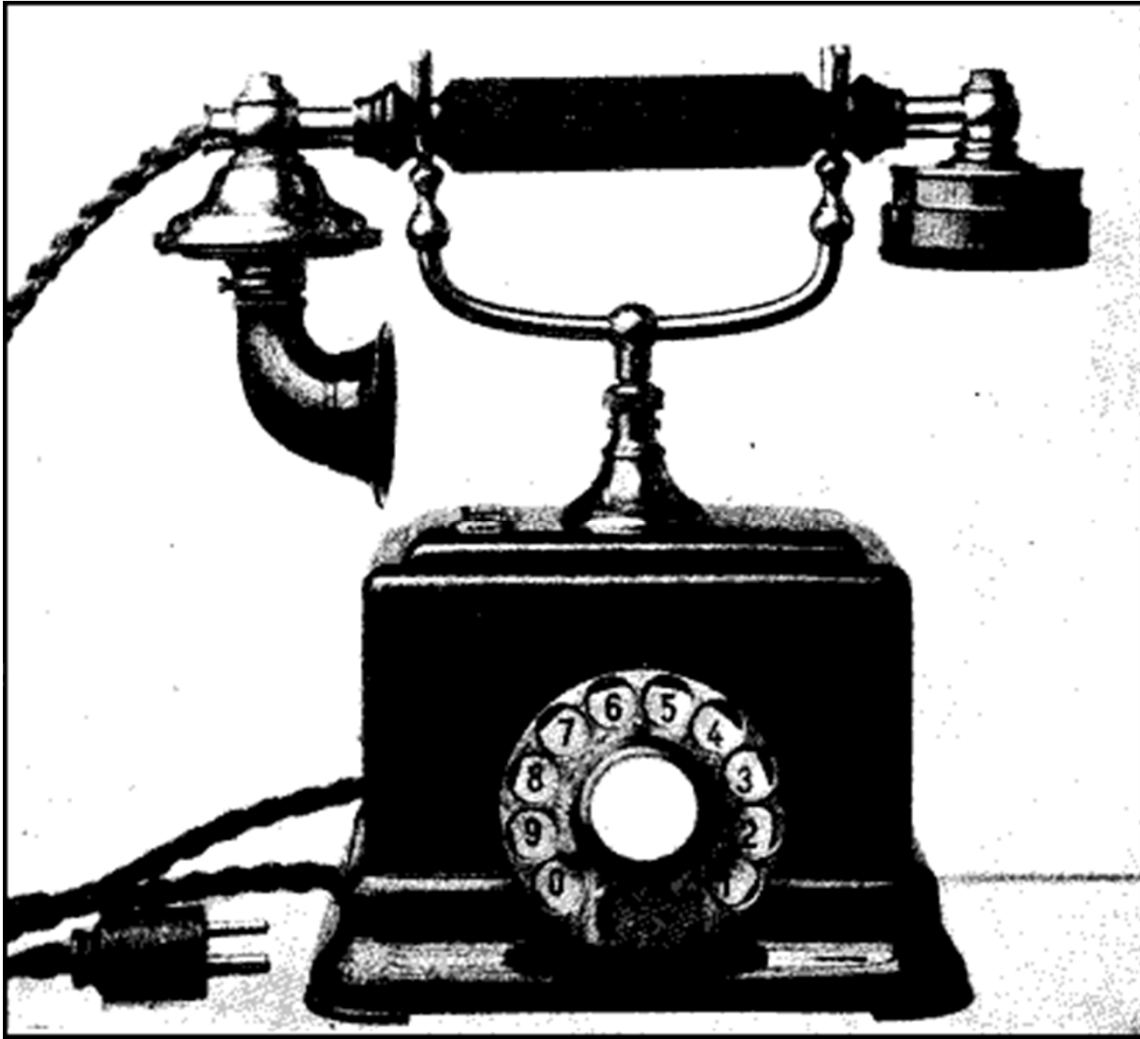
# What about data that leaves your possession?



Ex parte Jackson (1877) – 4th A applies to letters in transit



# Applying traditional rules to disruptive technology



Olmstead v.  
United States  
(1928) – 4th A  
does not apply  
to phone calls  
in transit



# Courts and Congress catch up

- 1967: Supreme Court – voice in transit protected
- 1968 – the federal Wiretap Act (aka “Title III”): sets out detailed procedures for issuing judicial warrants, based on probable cause, for real-time interception of “wire or oral” communications



# 1968 Wiretap Act limited in scope

- Only applied to the content of **voice** communications in transit **on a wire**. Didn't apply to:
  - Wireless voice
  - Data
- The courts in the 1970s said the 4th A didn't apply to:
  - Information disclosed to and stored by a third party
  - Non-content associated with communications





# Disruptive technology - a second wave

1969 - CompuServe founded - Internet introduces electronic and stored communications

1977 - Commercial cell phone service introduced





# Congress responds again - Electronic Communications Privacy Act 1986

- Required a warrant for all **real-time** access to content
  - Cell phone conversations
  - Email and other electronic communications
- Required court order for **real-time** access to dialed number information
- Allowed access without a warrant to some **stored** communications, as well as to subscriber-identifying info and other records



# Two new waves of disruptive technology

## “The Cloud”

- Under ECPA, many communications, documents and other items stored with a service provider are available to the government with a mere subpoena – no court order required, no probable cause of criminal conduct.

## Location

- ECPA allows access to “records pertaining to a subscriber” without a judicial warrant and without a finding of probable cause



# Warrant vs. subpoena - what's the diff?

UNITED STATES DISTRICT COURT  
CENTRAL DIVISION District of Utah

SEALED

In the Matter of the Search of  
(Name, address or brief description of person or property to be searched)

David Lacy  
[REDACTED]

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

Case Number: 2:09-MJ-212-A

I, PATRICK G. BROSANAN, being duly sworn depose and say:  
I am a Special Agent and have reason to believe that    on the person of or    on the premises known as (name, description and/or location)  
SEE ATTACHMENT A, attached to this application and incorporated herein by reference  
in the District of Utah there is now concealed a certain person or property, namely, (describe the person or property)  
SEE ATTACHMENT B, attached to this application and incorporated herein by reference  
which is (give alleged grounds for search and seizure under Rule 41(b) of the Federal Rules of Criminal Procedure)  
Believed to be property that constitutes evidence of the commission of a criminal offense and contraband, the fruits of crime or things otherwise criminally possessed.  
This application also seeks authorization for executing officers or agents to be accompanied by an archeologist or cultural artifacts expert, for the sole purpose of assisting agents in identifying and authenticating items to be seized, as contemplated in Attachment B of the Application and Warrant, incorporated by reference herein.  
Continued on the attached sheet and made a part hereof.   xx   Yes    No  
in violation of Title(s) 18 United States Code, Section(s) 16 U.S.C. § 470 ee, 18 U.S.C. § 641, 1163. The facts to support the issuance of a Search Warrant are as follows:  
See attached Affidavit incorporated by reference herein.  
Sworn to before me, and subscribed in my presence  
6/08/09  
Date  
SALT LAKE CITY, UTAH  
City and State  
SAMUEL ALBA, UNITED STATES MAGISTRATE JUDGE  
Name and Title of Judicial Officer  
Signature of Affiant  
Special Agent, FBI  
Signature of Judicial Officer

AC93/Rev 5/81 Search Warrant

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

In the Matter of the Search of

Residence at [REDACTED]  
Frederick, Maryland,  
owned by Bruce Edwards Ivins,  
DOB [REDACTED], SSN [REDACTED]

SEARCH WARRANT

CASE NUMBER: 07-524/M-01

TO: Postal Inspector Thomas F. Dellafera and any Authorized Officer of the United States

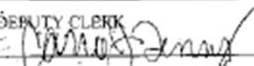
Affidavit(s) having been made before me by Postal Inspector Thomas F. Dellafera who has reason to believe that    on the person or    on the premises known as (name, description and/or location)

Single Family Residence at [REDACTED] Frederick, Maryland, and large white shed on rear of property, owned by Bruce Edwards Ivins, DOB [REDACTED], SSN [REDACTED]

in the District of Maryland there is now concealed a certain person or property, namely (describe the person or property)  
trace quantities of Bacillus anthracis or simulants thereof, hairs, textile fibers, lab equipment or materials used in preparation of select agents, papers, tape, pens, notes, books, manuals, receipts, financial records of any type, correspondence, address books, maps, handwriting samples, photocopy samples, photographs, computer files, cellular phones, phone bills, electronic pager devices, other digital devices, or other documentary evidence.  
I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.  
YOU ARE HEREBY COMMANDED to search on or before November 9, 2007  
(Date)  
(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search    (in the daytime - 6:00 A.M. to 10:00 P.M.)    (at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to the undersigned U.S. Judge/U.S. Magistrate Judge, as required by law.  
OCT 31 2007 5:08 PM  
Date and Time Issued in Washington, DC pursuant to the domestic terrorism search warrant provisions of Rule 41(b)(3)  
DEBORAH A. ROBINSON  
U.S. MAGISTRATE JUDGE  
Name and Title of Judicial Officer  
United States District Court  
For the District of Columbia  
A TRUE COPY  
NANCY MAYER WHITTINGTON, Clerk  
By [Signature]  
Deputy Clerk  
DEBORAH A. ROBINSON  
U.S. MAGISTRATE JUDGE



# And how does it compare with a subpoena?

United States District Court SOUTHERN DISTRICT OF INDIANA	
TO: Kristina Clair 4701 Pine St., Box 96 Philadelphia, PA 19143	SUBPOENA TO TESTIFY BEFORE GRAND JURY
SUBPOENA FOR: <input type="checkbox"/> PERSON <input checked="" type="checkbox"/> DOCUMENTS OR OBJECT(S)	
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.	
PLACE  U.S. Courthouse 46 East Ohio Street, 4th Floor Indianapolis, IN 46204	ROOM 464  DATE AND TIME February 24, 2009 9:30 a.m.
YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):	
SEE SUBPOENA ATTACHMENT	
In lieu of actual appearance before the Grand Jury, you may voluntarily waive your right to personally present the records and request a Special Agent to take custody of the documents to present to the Grand Jury. If you elect to do so, please complete the enclosed Waiver and Certification and forward it and your response before the date of compliance to the attention of:	
Task Force Officer Joel A. Arthur Federal Bureau of Investigation 575 N. Pennsylvania Street, Room 679 Indianapolis, IN 46204 Telephone: 317-639-3301	
<i>You are not to disclose the existence of this request unless authorized by the Assistant U.S. Attorney. Any such disclosure would impede the investigation being conducted and thereby interfere with the enforcement of the law.</i>	
This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court.	
CLERK LAURA A. BRIGGS, CLERK  (BY) DEPUTY CLERK 	DATE January 23, 2009 Arthur/kfb
This subpoena is issued upon application of the United States of America TIMOTHY M. MORRISON United States Attorney 09-01-DLP-15-10	NAME, ADDRESS AND PHONE NUMBER OF ASSISTANT U.S. ATTORNEY Doris L. Fryor Assistant United States Attorney 10 West Market Street, Suite 2100 Indianapolis, Indiana 46204-3048 (317) 226-6333
*If not applicable, enter "none."	



# The courts begin to respond

“[W]e hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP. ... The government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause.”

- Sixth Cir. Ct of Appeals, Dec. 2010 –  
“Warshak”



# The courts begin to respond - step 2

“The installation of a GPS device on a person’s car and the use of it to track the person over a prolonged period of time is a ‘search’ under the Fourth Amendment, which generally requires a warrant.”

US v. Jones, Supreme Court, Jan 2012





# Time for Congress to respond again

Updating ECPA – a convergence of interests:

- Service providers
- Users
- Government



# Digital Due Process

## Core Recommendations:

1. Judge's warrant for all content
2. Judge's warrant for location tracking
3. True judicial review for real-time access to transactional data
4. No blanket subpoenas for subscriber identifying data - must be particularized to subscriber or account – bulk requests must be upon judicial approval



# Digital Due Process Coalition

- Adobe
- Amazon.com
- AOL
- Apple
- AT&T
- CenturyLink
- Data Foundry
- Diaspora
- Dropbox
- eBay
- Facebook
- Google
- Hewlett-Packard
- IAC
- IBM
- Inflection
- IntegraTelecom
- Intel
- Intelius
- Intuit
- Linden Lab
- LinkedIn
- Loopt
- Microsoft
- Personal
- Salesforce.com
- TRUSTe
- American Booksellers Foundation for Free Expression
- American Civil Liberties Union
- American Library Association
- Association for Competitive Technology
- Association of Research Libraries
- Americans for Tax Reform
- Bill of Rights Defense Committee
- Campaign for Liberty
- Center for Democracy & Technology
- Center for Financial Privacy and Human Rights
- Citizens Against Government Waste
- Competitive Enterprise Institute
- Computer & Communications Industry Association
- The Constitution Project
- Consumer Action
- Distributed Computing Industry Association
- EDUCAUSE
- Electronic Frontier Foundation
- FreedomWorks
- Information Technology and Innovation Foundation
- The Joint Center for Political and Economic Studies
- Liberty Coalition
- National Workrights Institute
- NetCoalition
- Newspaper Association of America
- Software & Information Industry Association
- TechAmerica
- TechFreedom
- Telecommunications Industry Association



# Legislation Introduced

Leahy bill

GPS Act

Hearings in 2010  
and 2011



# Next Steps



**DIGITAL DUE PROCESS**  
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:**

- abf
- Aol.
- ACLU
- AMERICAN LIBRARY ASSOCIATION

**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 ►**

<http://www.digitaldueprocess.org>

