



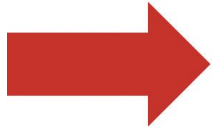
KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

CENTER FOR DEMOCRACY
& TECHNOLOGY

Cloud Privacy – ECPA & NSA

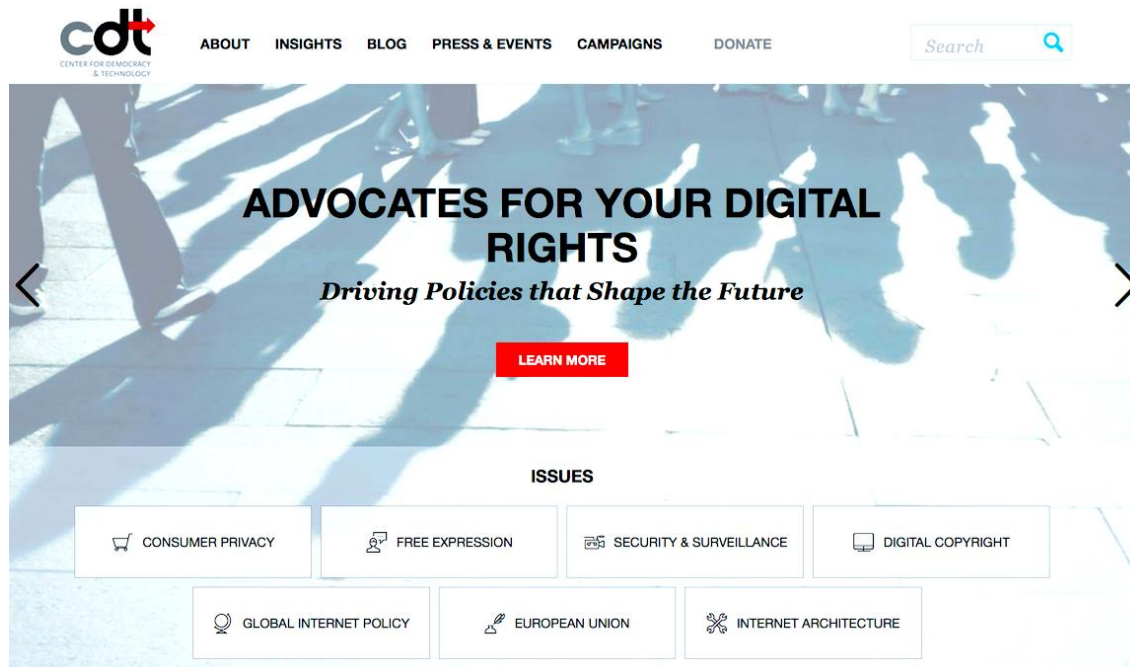
Mar. 26, 2015

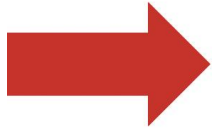
Harley Geiger
Senior Counsel
@HarleyGeiger



CDT.org

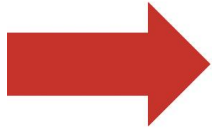
- Global nonprofit focused on technology and civil liberties.
- Privacy, free expression, Internet governance, innovation, and human rights.





Cloud computing is pretty neat, but what about government access to private data?

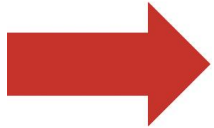
- Topic: Law enforcement access to digital content held in cloud by third party on behalf of users.
- Cloud computing depends on user trust in confidentiality of data.
- Warrant generally required for physical papers, files on a hard drive...
 - ...but not data stored in the cloud!



ECPA, class of 1986

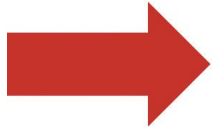
- The Electronic Communications Privacy Act of 1986
- Specifies standards for government access to data stored with service providers on behalf of users.





ECPA standards

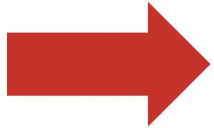
- Cloud content under 180 days old: Warrant.
 - But not if the message content has been opened...
 - ...except in the 9th Circuit.
- Cloud content over 180 days old: Subpoena or “d order” plus user notice.
 - But not in the 6th Circuit – warrant required.
- State laws
 - Missouri, Texas...



Tech evolved – so should ECPA

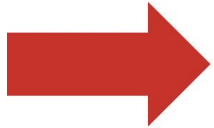


- Incompatible with modern business practices.
- Contrary to user expectation of privacy.
- Difficult for companies, courts, and legislatures to apply.



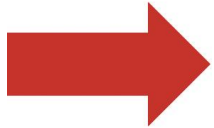
ECPA reform proposals

- Flat warrant standard, regardless of age or status.
- Digital Due Process Coalition:
 - ACLU, Amazon, Americans for Tax Reform, Apple, AT&T, BSA, CCIA, CDT, Dell, Dropbox, eBay, Facebook, FreedomWorks, Google, HP, IBM, Intel, LinkedIn, Microsoft, SIIA, Snapchat, SpiderOak, T-Mobile, Twitter, Tumblr, Yahoo... etc...
 - DigitalDueProcess.org
- Email Privacy Act – H.R.699
 - Leadership



Microsoft Ireland

- Can US law enforcement compel a US cloud provider to disclose digital content stored outside the US?
- Microsoft: Search occurs where data is located
- DOJ: Warrant applies to party controlling data
- Risk of other governments making extraterritorial demands
- Risk of data localization
- MLATs
- LEADS Act



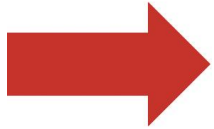
NSA



SSL Added
and removed
here! 😊



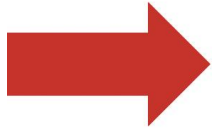
KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE



NSA reforms

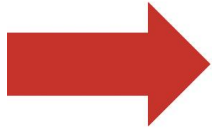
- Legislation in advance of Sec. 215 sunset
- Bulk collection
 - Metadata, not content
 - Sec. 215 and FISA pen/trap
- Transparency
 - Content and metadata
- FISA Court
- PRISM?
- Precedent





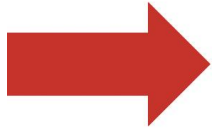
Conclusion - ECPA

- Cloud data receives weaker protection than physical items and data stored locally.
- Current laws – ECPA – are badly outdated and contrary to Fourth Amendment principles.
- ECPA reform proposals on the table: Digital Due Process coalition, Email Privacy Act, LEADS Act



Conclusion - NSA

- Congress will consider reform legislation in the next 8-10 weeks.
- Legislation likely to cover bulk collection, transparency, FISC reform.
- Strength of the reforms and the amount of support will set stage – for better or worse – for future reforms.



Thank you!

Harley Geiger

Senior Counsel, CDT

@HarleyGeiger

cdt.org