Legal cooperation to overcome jurisdictional and territorial limits in cybercrime investigations

Craig Ng
General Counsel, APNIC

National laws confined to territorial limits

<< Borderless Internet >>

- Ransomware
- DoS and DDoS Attacks
- Malware Attacks
- Phishing Attacks
- Business E-Mail Compromise (BEC)
- Data Breaches and Leaks
- Cryptojacking


WannaCry
WannaCry
WannaCry
WannaCry

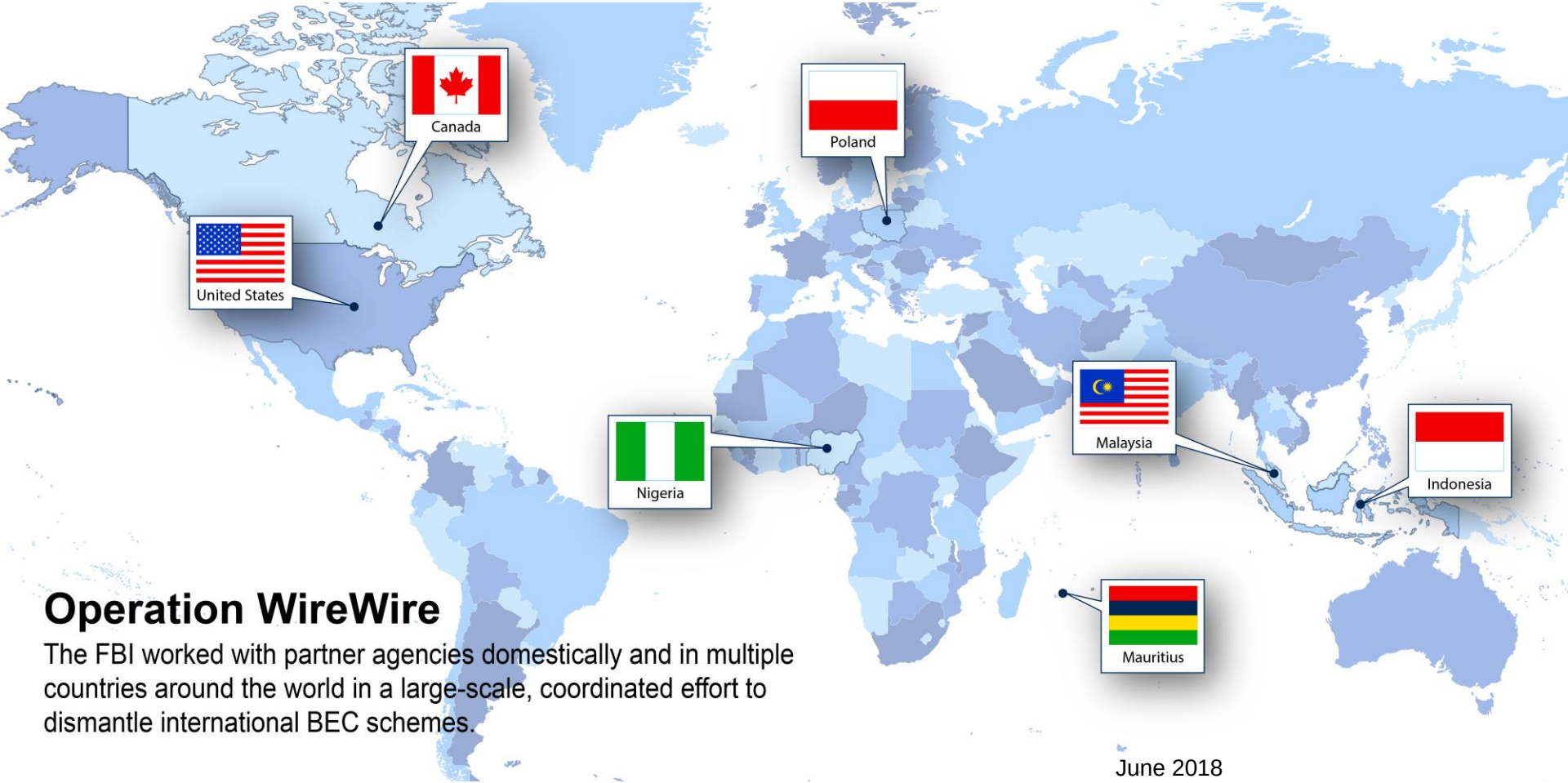
In May 2017:

- Global cyberattack
- Ransomware virus affected 150 countries
- Crippled British healthcare system
- More than 19,000 medical appointments cancelled
- Blocked access to computer systems managing 600 surgeries
- Ambulances redirected routes from five hospitals

- Attack was stopped after discovery of “kill switch”
- New variant in August 2018 forced *Taiwan Semiconductor Manufacturing Company* to shut down temporarily

Cross-Border Internet

National Laws and Jurisdictions

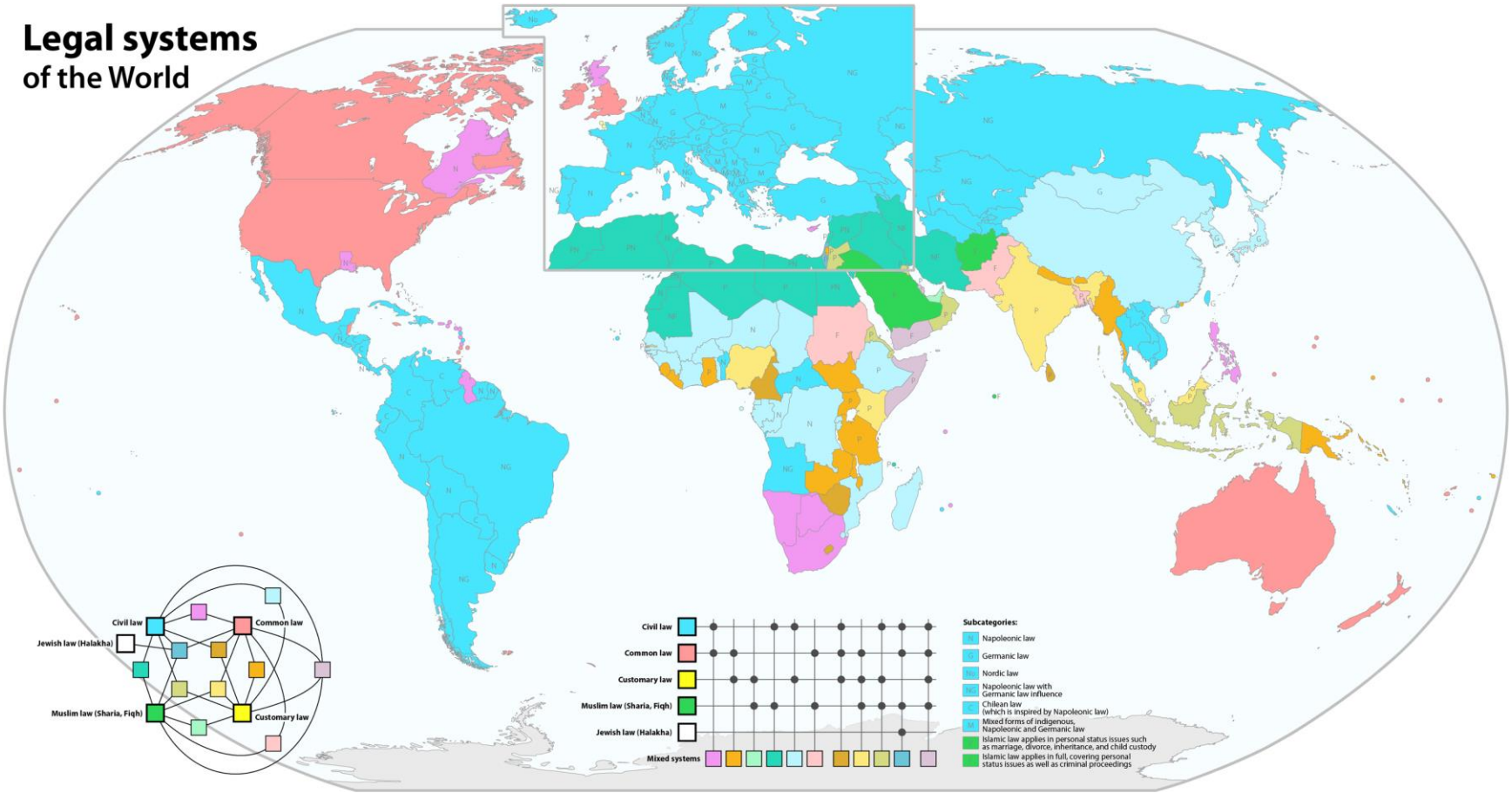


Operation WireWire

The FBI worked with partner agencies domestically and in multiple countries around the world in a large-scale, coordinated effort to dismantle international BEC schemes.

June 2018
Source: US Department of Justice and FBI

Legal systems
of the World

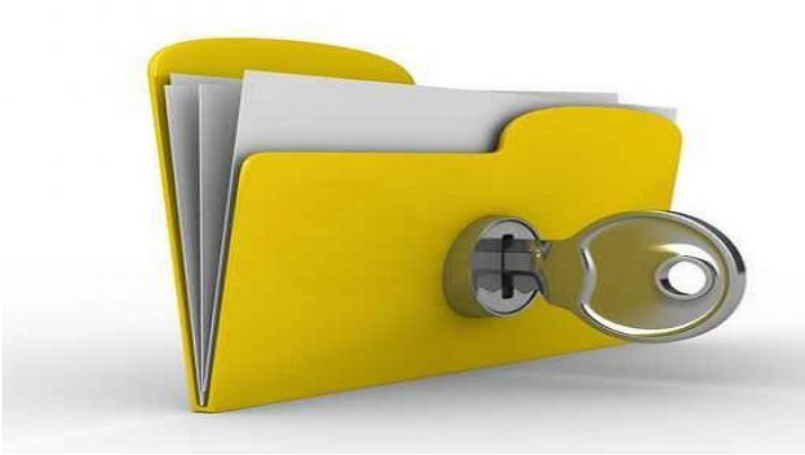


Criminal Investigations

- *Need to access information about users and digital evidence*
- *Usually stored by private companies in jurisdictions outside of investigating country*
- *Sometimes difficult to determine location and connection with particular jurisdiction*

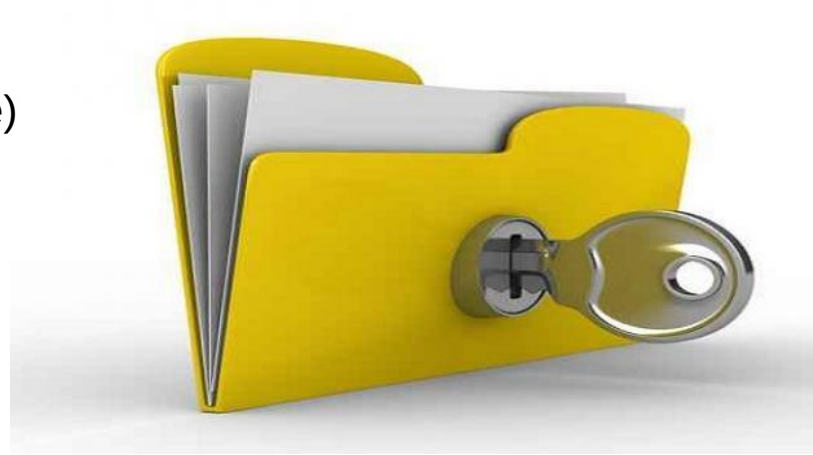
Challenges to Accessing Cross-Border User Data

- Necessary compliance with transnational due process mechanisms (to prevent abusive access)
- Conflicts of laws between jurisdictions
- “Needle in the haystack” with large volume of data collection
- Large-scale deployment of end-to-end encryption
- Privacy laws



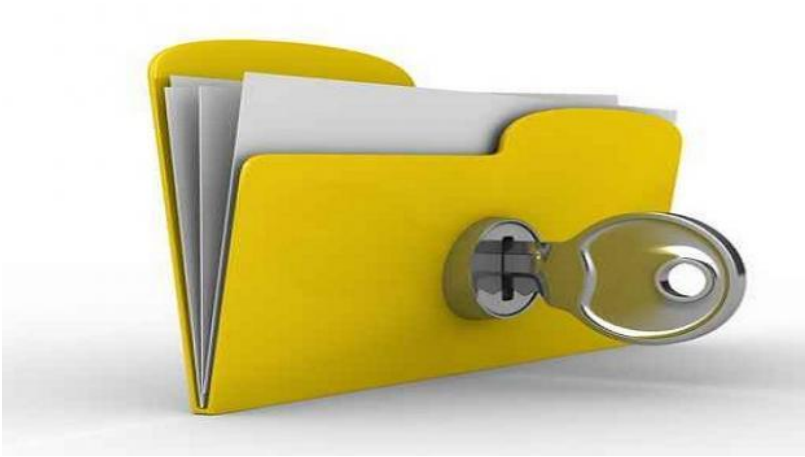
Current Solutions

- **MLAT** (Mutual Legal Assistance Treaties)
- **Budapest Convention** (Convention on Cybercrime)
  - *Slow and complex*
  - *Not scalable to all countries*
- **Legal Cooperation**
  - *Lacks transparency*
  - *Depends on private network of law enforcement agencies*
  - *Questions around admissibility of evidence*
  - *Conflicts of laws*



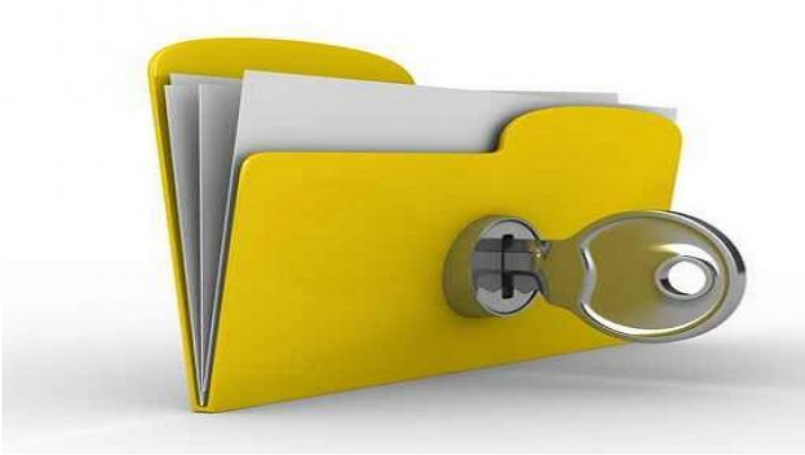
Legal Cooperation Networks

- **INTERPOL**
  - Member countries host NCB (National Central Bureau)
  - Network called I-24/7
  - NCBs work with law enforcement agencies in their own country and other NCBs around the world
  - NCBs contribute crime data to global databases



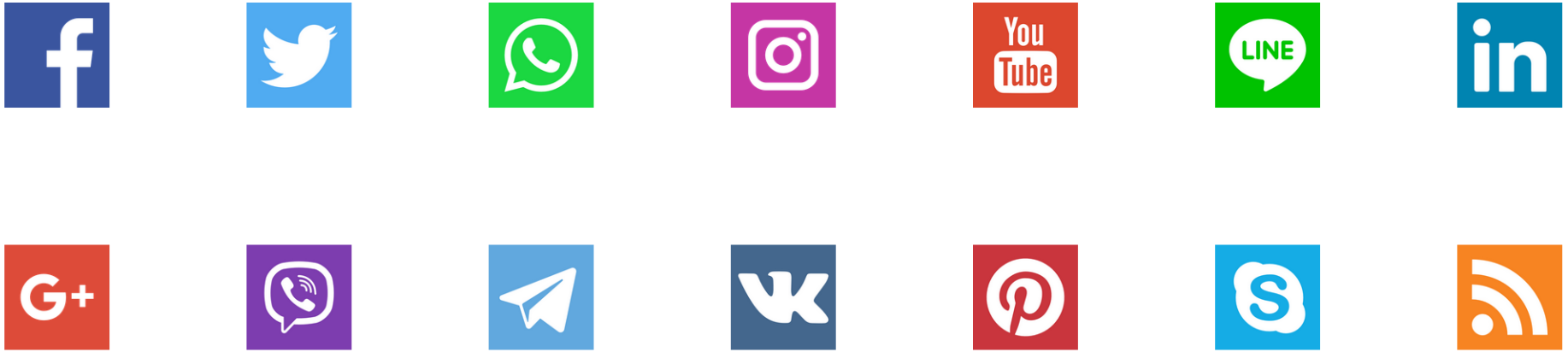
Legal Cooperation Networks (continued)

- **G7 24/7 High Tech Crime Network**
  - G7 = Group of Seven
  - Network includes more than 70 countries
  - Exists to ***preserve*** digital evidence for subsequent transfer through legal channels
  - Member countries create a single point-of-contact available to other member nations, 24 hours per day/7 days per week

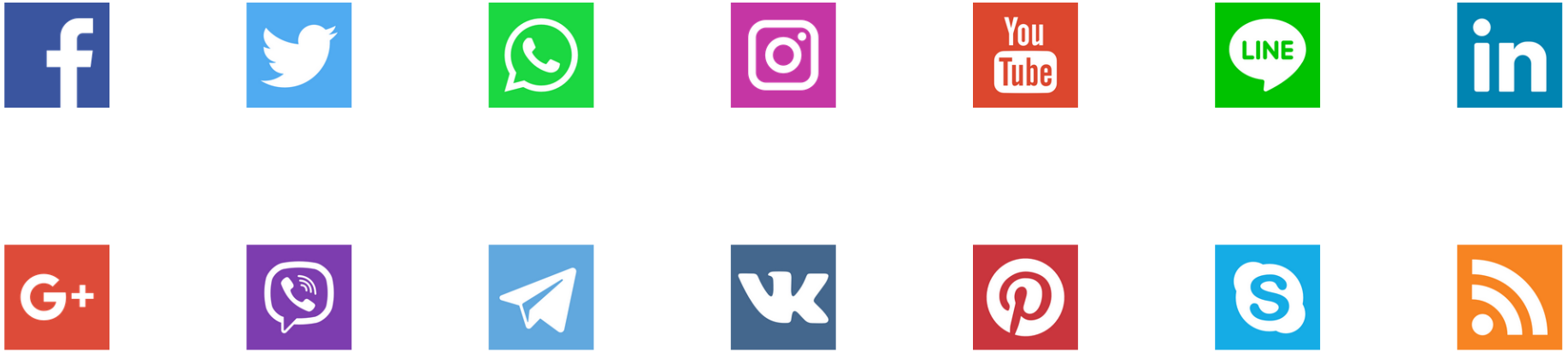


Problems with legal cooperation

- *Conflicting laws for voluntary cross-border cooperation and disclosures*
- *Complying with laws of one country can break the laws in another country*


You
Tube
LINE

Many technology companies are based in United States



facebook

Law Enforcement Online Requests

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

☐ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the Law Enforcement Guidelines.

English (US) English (UK) 中文(简体) 한국어 日本語 Français (France) Español Deutsch Italiano Português (Brasil) العربية +

Sign Up Log In Messenger Facebook Lite Watch People Pages Page Categories Places Games Locations Marketplace Groups Instagram
Local Fundraisers Services About Create Ad Create Page Developers Careers Privacy Cookies Ad Choices Terms Help

CLOUD Act

- **CLOUD = Clarifying Lawful Overseas Use of Data Act**
- US federal law enacted in March 2018 – it amended the US *Stored Communications Act* (SCA)
- Clarification needed following the *Microsoft case* – where US Federal Court decided that SCA does not require Microsoft to disclose information in its custody and control that it stored on a server in Ireland

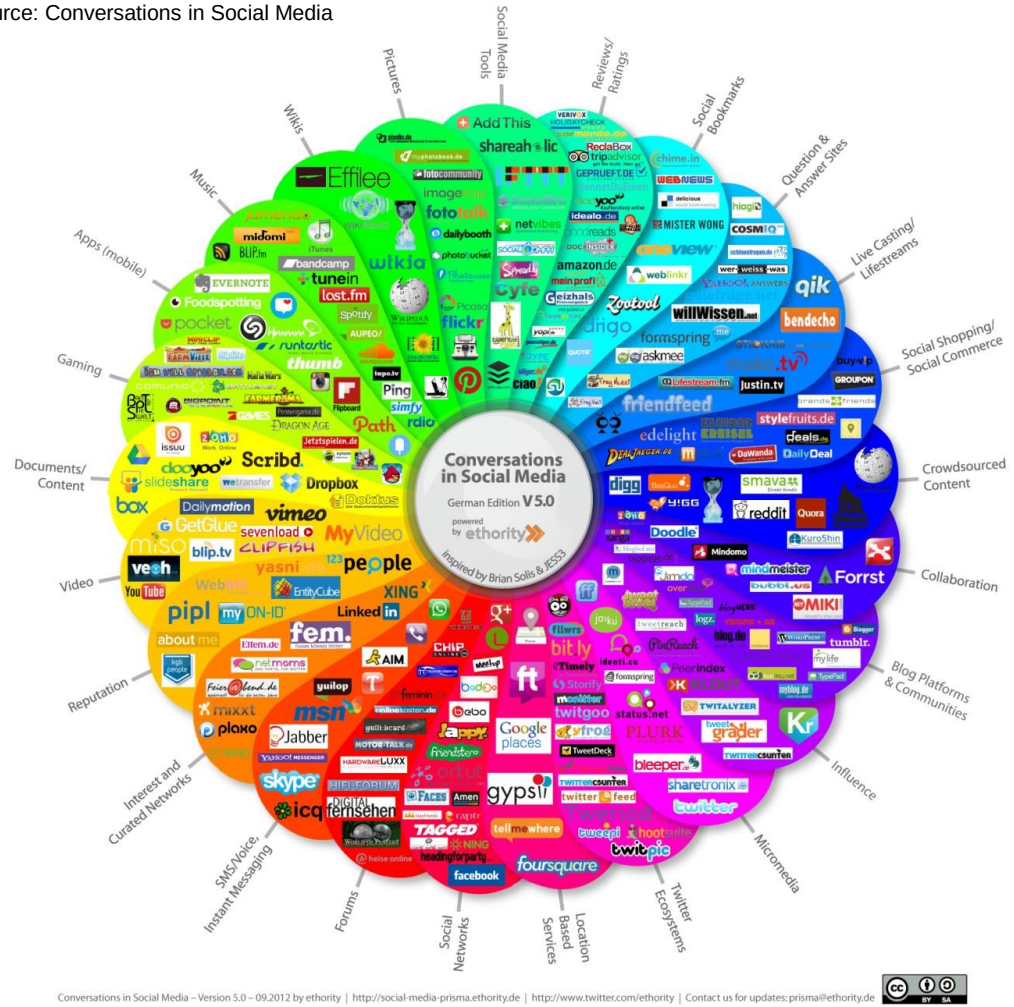
CLOUD Act

- Allows US law enforcement agencies to compel US-based technology companies to provide requested data, ***even if stored outside US***
- Removes potential conflict of laws, lifts restrictions under US law on US companies disclosing electronic data ***to foreign authorities*** in investigating serious crimes
  - If foreign countries sign “CLOUD Act Executive Agreements” with US
  - To be eligible, foreign countries must establish appropriate standards and checks and balances within its legal framework to protect privacy, civil liberties, and human rights
  - “CLOUD Act Executive Agreements” also allow US authorities to seek electronic data from *foreign* technology companies if supported by US warrants

What about OSINT?

“OPEN-SOURCE INTELLIGENCE”

Source: Conversations in Social Media



Open-Source Intelligence (OSINT):

- *Using **publicly available** sources to collect information from a wide array of sources (including the Internet)*

Conclusions and way forward

- ***Participate in existing law enforcement networks*** (INTERPOL + G7 24/7) to assist in investigations and request preservation of data
- ***Make use of Mutual Legal Assistance Treaties/Agreement*** (MLAT/MLAA) for evidence collection
- ***Make use of the Budapest Convention*** (Convention on Cybercrime of the Council of Europe) for evidence collection
- ***Make use of Open-Source Intelligence*** for intelligence gathering
- Consider bilateral ***Executive Agreement under CLOUD Act***

Questions?