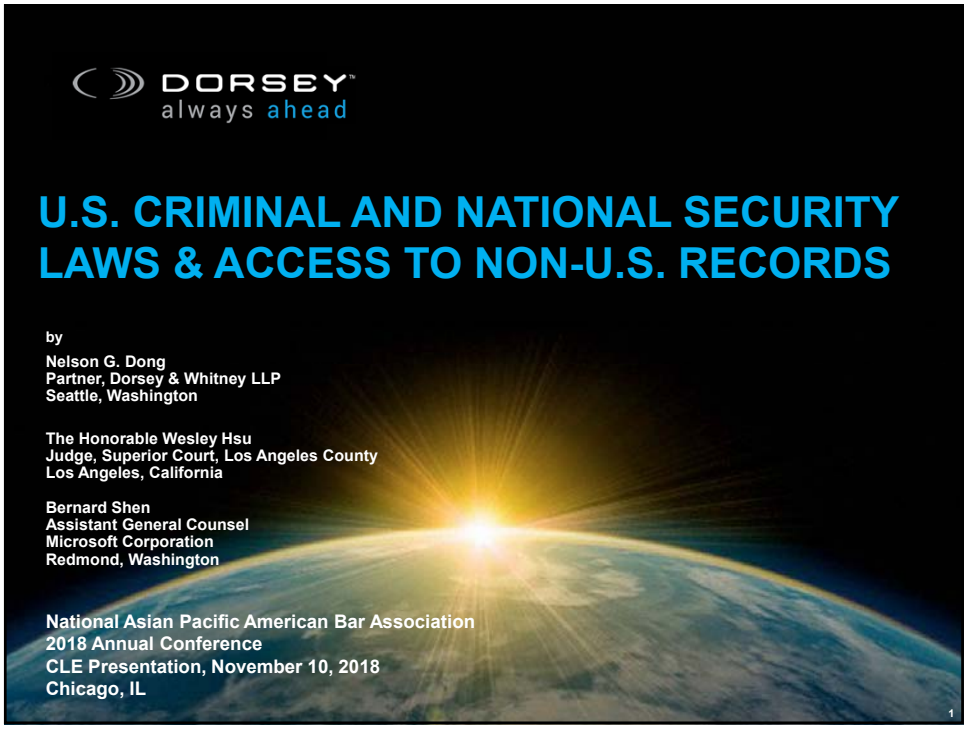


PROFESSIONAL BACKGROUNDS

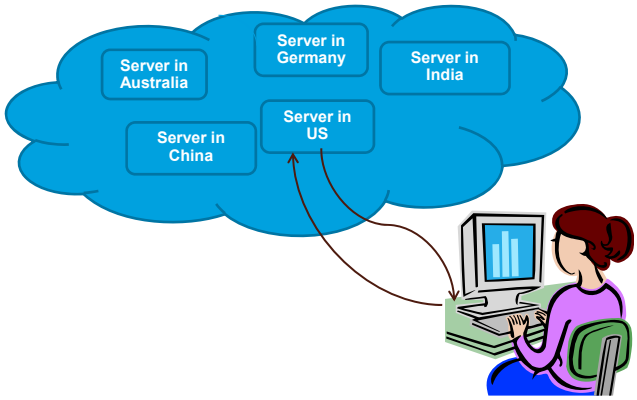
- **NELSON DONG: Dorsey's National Security Law Group head & Asian Law Group co-head; U.S. export controls, national security issues in international business transactions; former U.S. Justice Department official with national security roles; former AUSA (Criminal Division) in Boston.**
- **WESLEY HSU: Judge, Los Angeles County Superior Court; former Deputy U.S. Attorney, Exec. Asst. U.S. Attorney & AUSA in Central District of California; former Cyber & IP Crimes Unit head; personally prosecuted many "first time" computer-related criminal cases; has taught criminal law at Loyola University Law School.**
- **BERNARD SHEN: Assistant General Counsel, Microsoft Corporation; helps to frame company's defense of freedom of expression, privacy and human rights, including protection of user information & records across all product and service lines; lead attorney for CLOUD Act issues**

WHAT IS "THE CLOUD"?

U.S. Department of Commerce's National Institute of Science and Technology (NIST) defines "cloud computing" as:

"… a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisions and released with minimal management effort of service provider interaction."

HOW DOES THE CLOUD WORK?



Data moves within a cloud to adjust to computing capacity within various servers constituting the cloud.

Cloud looks the same to the user – movement of data is seamless and untraceable to user.

4th AMENDMENT & SEARCHES

- **U.S. Constitution's Bill of Rights includes famous Fourth Amendment:**

  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 Warrant 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.

- **Many U.S. court decisions have held:**
  - **Companies are "persons" protected by 4th Amendment**
  - **Company business records may be "searched and seized" by means of search warrants issued to FBI, other federal officers**
  - **U.S. District Court judges, magistrate judges may issue such search warrants consistent with 4th Amendment standards**

INFORMATION TECHNOLOGY & "RECORDS"

- **U.S., as common law jurisdiction, has had over 200 years of judicial case law on application of 4th Amendment to "*searches and seizures*" of traditional paper-based business records**
- **Today, most companies rely on both paper and, increasingly, *electronic* or digital business records**
  - **Electronic records can now be stored on multitude of devices and systems and in multiple jurisdictions**
  - **Records may be on mobile phones; on personal computers; on local area network via servers; on leased 3rd party servers; or, increasingly, stored and used "in the Cloud"**
  - **"Enterprise"-wide IT means potential technical access to electronic records even when storage medium is outside U.S. jurisdiction**
- **U.S. case law continues to evolve as legal principles applied once only to paper records are being adapted, reshaped to fit new era of electronic records**
  - **Globalization of business and of IT are breaking new ground on how to apply 4th Amendment law to *foreign* business records**

HISTORIC LIMITS TO U.S. JURISDICTION

- Generally speaking, U.S. investigators, prosecutors have no jurisdiction outside United States
- Traditional method of "international" law enforcement is by means of mutual legal assistance treaties (MLATs)
  - Antigua & Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, Germany, Greece, Grenada, Hong Kong, Hungary, India, Ireland, Israel, Italy, Jamaica, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Mexico, Morocco, the Kingdom of the Netherlands (including Aruba, Bonaire, Curacao, Saba, St. Eustatius and St. Maarten), Nigeria, Panama, Philippines, Poland, Romania, Russia, St. Lucia, St. Kitts & Nevis, St. Vincent & the Grenadines, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Trinidad & Tobago, Turkey, Ukraine, United Kingdom (including the Isle of Man, Cayman Islands, Anguilla, British Virgin Islands, Montserrat and Turks and Caicos), Uruguay, and Venezuela
  - US-EU convention gives U.S. legal ties to every EU member nation
- U.S. is also bound by OAS Convention on Mutual Legal Assistance, UN Convention against Corruption, UN Convention against Transnational Organized Crime, International Convention for Suppression of Financing of Terrorism and UN Drug Convention

"POSSESS OR CONTROL" STANDARD

- However, U.S. courts have traditionally ruled that domestic search warrants can be served on U.S. company and compel production of records held by such company's foreign affiliate
  - Usual test: does U.S. company "possess or control" records?
  - "*Control*" is usually multi-part factual determination by judge:
    - Common ownership of entities
    - Common directors, officers, employees among entities
    - Routine exchange of documents between U.S. entity and foreign entity in normal course of business affairs
    - Benefits accruing to foreign entity from conduct of U.S. entity
    - Involvement of foreign entity in conduct of U.S. entity
  - Easiest case: U.S. parent entity and 100% owned foreign subsidiary or foreign branch office
  - But U.S. subsidiary or joint venture, based on above factors, might be held liable to produce records of its foreign parent too

U.S. JUDICAL SEARCH WARRANTS & NON-U.S. BUSINESS RECORDS

- **Historic U.S. Department of Justice position: may use domestic U.S. search warrant to demand that a U.S. company must deliver *non-U.S.* (e.g., European) business records**
  - **Well established U.S. legal principle about U.S. company's duty if it "possesses or controls" foreign business records being sought**
- **Major challenge in *Microsoft Corp*. v. *USA* litigation in 2014-18**
  - **2014: U.S. District Court in SDNY issued domestic search warrant to Microsoft, demanding customer's emails stored only on Microsoft's email servers in Ireland**
  - **Microsoft admitted it has technical ability to access such Irish emails from its U.S. facilities, with no technical action needed within Ireland**
  - **Microsoft opposed warrant, arguing (a) such a "domestic" warrant has unlawful extraterritorial effects and (b) U.S. Government should apply under MLAT with Government of Ireland to gain access to such emails stored in Ireland**
  - **Government of Ireland itself filed *amicus curiae* brief in case, restating its willingness to adhere to MLAT to assist U.S. criminal investigation if asked (but did not argue merits of whether warrant was illegal under U.S. law)**
  - **2016: 2nd Circuit Court of Appeals reversed and quashed search warrant**
  - **2017-2018: U.S. Supreme Court granted *certiorari* but dismissed as moot when both parties sought dismissal of appeal in light of new CLOUD Act legislation**

CLOUD ACT

- ***C*larifying *L*awful *O*verseas *U*se of *D*ata Act ("CLOUD Act") passed in March 2018 as Section 105 in Consolidated Appropriations Act, Pub. Law 115-141**
  - **Unusual method of passage avoided any testimony, committee hearings or separate Congressional vote on CLOUD Act**
- **Mainly amends 1986 Stored Communications Act ("SCA") to permit federal law enforcement agencies to compel U.S.-based technology companies through search warrants or grand jury subpoenas to provide data stored on their servers, *regardless of location***
  - **Justice Department, Microsoft both agreed CLOUD Act rendered their case before U.S. Supreme Court as moot, resulting in dismissal of entire case from federal courts**
- **Also authorizes U.S. Government to negotiate MLAT-type executive agreements with other national governments on law enforcement access to digital data and records**
- **Despite CLOUD Act now being "*the law*," still many divergent views on whether Congress acted wisely in view of historic value placed on protection of personal privacy**

DECEMBER 2016 AMENDMENT TO RULE 41, FEDERAL RULES OF CRIM. PROCEDURE

- **At Justice Department request, U.S. Supreme Court proposed in April 2016 and made effective in December 2016 certain technical amendments to Federal Rules of Criminal Procedure**
- **One change affected Rule 41 in regard to execution of judicial search warrants:**

  ... a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

  (A) the district where the media or information is located has been concealed through technological means; or

  (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.
- **Amendment was opposed by many U.S. technology companies, especially ISPs, common carriers**
  - **Fearful of more U.S. Government demands on foreign business records, collisions with privacy protection laws (e.g., in E.U.)**
  - **Change in Rule 41 language should be taken together with new CLOUD Act**

FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC)

- **Special U.S. federal court for foreign intelligence cases**
  - **Established originally under historic 1978 Foreign Intelligence Surveillance Act (FISA), so often called in media the "FISA court"**
  - **Created means of judicial supervision over what had previously been warrantless searches of *foreign* persons by Federal Bureau of Investigation (FBI) and National Security Agency (NSA)**
  - **Based in Washington DC**
  - **Comprised originally of seven U.S. District Court judges appointed by Chief Justice of United States; expanded in 2001 to panel of 11 judges**
  - **All proceedings of FISC are *ex parte* and in secret with only U.S. Department of Justice lawyers appearing for FBI and NSA**
- **FISC has ruled *content* of electronic or other forms of communication (voicemails, email, letters) are protected under U.S. Constitution's 4th Amendment, requiring judicial search warrant to be searched and seized**
- **FISC has also ruled *metadata* are *not* protected under 4th Amendment**
  - **Metadata includes phone numbers, IP addresses, time, date, duration and frequency of communications**

USA PATRIOT ACT

- ***U***niting and ***S***trengthening ***A***merica by ***P***roviding ***A***ppropriate ***T***ools ***R***equired to ***I***ntercept and ***O***bstruct ***T***errorism Act
- Originally passed in 2001 as Pub. Law 107-56 to amend multiple parts of U.S. Code (across multiple titles)
- Strong bipartisan measure taken after 9/11 tragedies
  - Justice Department draft in 19 September House bill
  - House vote on 24 October: 357 − 66
  - Senate vote on 25 October: 98 − 1
- Promptly signed, used by President George W. Bush
  - Despite original "sunset" and criticisms, Congress extended law again in '04, '06, '09, '11

MANY OTHER FEDERAL LAWS AFFECTED

- USA PATRIOT Act's main effect was to reduce degree of personal privacy protection in certain national security investigations
- Expanded U.S. Government access to multiple kinds of business records covered by various U.S. privacy protection laws, such as:
  - Foreign Intelligence Surveillance Act
  - Electronic Communications Privacy Act
  - Bank Secrecy Act
  - Right to Financial Privacy Act
  - Fair Credit Reporting Act
  - Family Educational Rights & Privacy Act
  - Immigration and Nationality Act
  - Stored Communications Act (as amended by CLOUD Act)

BASIC TITLES IN USA PATRIOT ACT'S STRUCTURE

- I: Enhanced domestic security services
- *II: Enhanced surveillance procedures*
- III: Anti-money laundering measures
- IV: Border security measures
- V: Removing obstacles to terrorism investigations
- VI: Victims, families of victims
- VII: Increased information sharing for critical infrastructure protection
- VIII: Terrorism criminal law changes
- IX: Improved intelligence
- X: Miscellaneous

TITLE II'S EXTENSIVE FEATURES

- Allows gathering of "foreign intelligence information" from both U.S. citizens and non-citizens
- Allows FISA court surveillance to be ordered where "foreign intelligence" is only "significant" but not "primary" purpose, as it had to be before the Act
- Expanded duration of FISA searches, surveillance
- Allows wiretaps to include Internet addressing, routing
- Allows search warrant access to stored voicemail
- Allows owners/operators of "protected computers" to consent to message interception without need for wiretap
- Expanded ISP account data open to federal agents

NATIONAL SECURITY LETTERS

- **NSL: administrative subpoena from FBI agent**
  - **First authorized by Congress in 1986**
  - **Currently must be approved by senior official at FBI HQ or by Special Agent in Charge of FBI field office**
- **When NSL sent to ISPs or common carriers, may seek only metadata (non-content data)**
  - **E.g., IP addresses, phone numbers, times, dates, etc.**
  - **Generally speaking, NSL seeks clarifying data on "*who is in contact with whom*"**
- **Almost all FBI NSLs have "gag order" barring ISP, telecomm carrier or banks from disclosing to its customer that NSL was issued, usually with no time limit on that bar**
  - **2008 Inspector General audit finding: 97% of NSLs had gag order**
  - **Recent amendment does allow recipient of NSL to consult with legal counsel about scope, effect of NSL**

INCREASING USE, EFFECT OF NSLs

- **Federal Bureau of Investigation (FBI) has reported issuing fewer NSLs but making more requests for information in NSLs sent to U.S. ISPs, common carriers, banks and other holders of business records**
  - **2014: 16,348 NSLs issued by FBI containing 33,024 data requests**
  - **2015: 12,870 NSLs issued by FBI containing 48,642 data requests**
- **Each data request may seek someone's email or IP addresses, phone numbers, account data, other metadata**
  - **In 2015, FBI made 31,863 requests via NSLs for records related to 2,503 foreign persons**
  - **Increase attributed mainly to ISIL recruitment in U.S. across multiple social media platforms**
- **U.S. and international IT industry increasingly opposed to NSLs with indefinite gag orders**

CONCLUSION

- Ever-greater international criminal activity and international terrorism are enabled by the Internet, modern IT systems, leading to more intrusive surveillance, expanded investigations by law enforcement and national security authorities
- FBI, other agencies will rely on traditional MLATs where appropriate but will also to use search warrants, NSLs and other means to access metadata and business records of foreign persons, including some electronic records stored and processed outside United States, if "controlled" by a U.S. company
  - U.S. statutes evolving (e.g., FISA, USA PATRIOT Act, etc.)
  - U.S. court decisions also still being shaped
- *Microsoft Corp. v. USA* case tried to challenge permissible scope of U.S. judicial domestic search warrants to access foreign-stored electronic records; new CLOUD Act legislation mooted case before Supreme Court could render own view
- Amended F.R. Crim. Pro. Rule 41 may already signal U.S. Supreme Court views long-standing "*possess or control*" rule as including foreign electronic records technically accessible from within U.S.

THANK YOU!

NELSON G. DONG

Dorsey & Whitney LLP
Columbia Center
701 Fifth Avenue, Suite 6100
Seattle, Washington 98104-7043

Phone: (206) 903-8871
Fax: (206) 260-9085
Email: dong.nelson@dorsey.com