RSAConference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: CMI1-F03

Encryption, Apple, and Global Implications

Jeffrey J. Blatt

Of Counsel
Tilleke & Gibbins International
Bangkok, Thailand
Twitter: @TechLawExpert

#RSAC

1984
WAS
NOT
SUPPOSED
TO BE AN
INSTRUCTION
MANUAL

Our Objectives In This Session

- Understand the US v. Microsoft case, the recent U.S. court of appeals decision, and its business and personal data privacy ramifications for data stored in transnational Clouds
- Understand the FBI v. Apple Case and its ramifications for data stored at the digital device level
- Explore the US Government's 'Nowhere To Hide' strategy to reach data stored on any device in its possession, or stored in any Cloud anywhere on earth
- Discuss the global implications of the US approach and some possible strategies to mitigate

Background:
Encryption and the Keys to the City

Driven by the Snowden leaks, the exponential increase in cyber attacks and customer demands for better digital security and privacy, the tech industry is embracing encryption and major service providers like Microsoft and Apple have added end-to-end encryption of data they host and manage including data stored in Clouds and on digital devices:

- A *fundamental* question to ask is who controls the decoding keys (e.g. the service provider or the data owner/customer)?
- If the the service provider or device manufacturer holds the keys, data sought by the government through legal process can be provided.
- IF the customer holds the keys, and a government wants access to the customer's data, it would need to go to the customer directly. The Cloud service provider can only be compelled to provide what it has (encrypted data), and the device manufacturer similarly cannot provide access to the data on the device and/or provide decrypted data. **This is a 'key' issue (*pun intended*)**

More Preliminaries -> The Third Party Doctrine under US Law

- “**Third Party Doctrine**”: As a matter of US Fourth Amendment law there is no expectation of privacy to a vast amount of our personal data shared with 3rd parties. Absent specific legislation no warrant required, just a simple subpoena is needed (much lower threshold)
  - Examples: Your Waze history, Siri interactions, banking statements and medical data records, email metadata, websites visited, phone records and cell tower location data, education records…and much much more…

United States v. Microsoft

- *THE most important case currently pending affecting Cloud based services and the industry today –*
- Microsoft challenged a U.S. search warrant seeking access to customer emails stored in Dublin, Ireland. District court issued the warrant, and ruled in favor of the U.S. Microsoft appealed to the Second Circuit. On July 14th 2016 a 3 judge panel of the Court of Appeals <u>decided in FAVOR</u> of Microsoft.
- Amicus briefs filed in support of Microsoft's position by 28 technology companies, 23 trade groups, 35 computer scientists and the Irish government.

United States v. Microsoft (con’t)

- Fact Summary: The U.S. obtained a search warrant issued under the Stored Communications Act issued by the U.S. Dist. Ct (SDNY) for information (emails of a customer) stored at premises ‘owned, maintained, controlled or operated by Microsoft Corporation’
- In fact, while some of the data sought by the U.S. is stored in the U.S.A. (e.g. address book) the emails are stored in Microsoft’s Irish data center (‘cloud’) owned and controlled by Microsoft U.S.A.
- Microsoft U.S.A. has objected to having to compel its Irish subsidiary to search, seize and disclose – likely in violation of Irish law – the information sought by the U.S. government in the warrant.
- Microsoft asserts that U.S. search warrants cannot reach its overseas operations, and also that the U.S. should seek the information via a Mutual Legal Assistance Agreement (MLAT) in place with Ireland. The 2nd Circuit Court of Appeal AGREED with Microsoft

United States View of Jurisdiction

- The government’s case is straightforward -
- Microsoft owns and controls the Irish subsidiary and has within its power the ability to compel the Irish subsidiary to provide the information (albeit perhaps in violation of Irish law).
- The U.S. Department of Justice takes a very broad view of U.S. jurisdiction.
  - In various cases including Microsoft, but also FCPA, Export Control, Banking, Money Laundering, Iran Sanctions, U.S. Tax Evasion….
    - One email through a U.S. server is sufficient to establish an ‘act’ in the U.S.A.
    - Use of United States Dollars via a transfer through a U.S. correspondent bank
    - U.S. parent company control over a foreign subsidiary
    - Regardless of local laws applicable in the foreign jurisdiction

Microsoft: The U.S. Government's Strategy -

- The U.S. Government's objective:
  - to establish that any cloud service provider within the jurisdiction of the U.S. must comply with a U.S. issued search warrant *regardless of where the data sought is stored and notwithstanding local country law where the data is stored*
- As such, a U.S. search warrant would effectively have worldwide application. Note that the 2nd Circuit's decision only applies in that Circuit. Only a U.S. Supreme Court decision would apply over the entire U.S.
- In furtherance of this objective the FBI has successfully lobbied to amend Rule 41 of the US Federal Rules of Criminal Procedure

Microsoft's Business Response (Part 1)

- While awaiting a decision by the 2nd Circuit Court of Appeals, Microsoft tried a different and imaginative approach to limit the business and reputation damage caused by the US government's nowhere to hide strategy -

- Germany has been very upset by the Snowden Disclosures

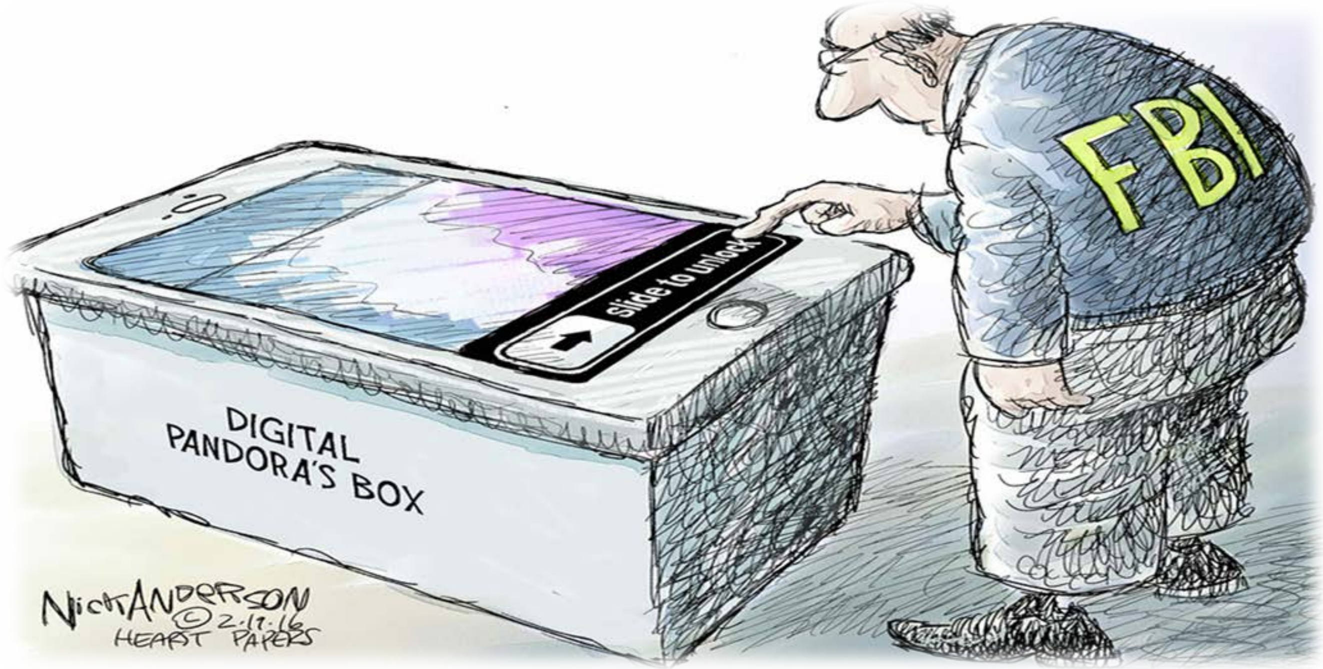
- On November 11, 2015, Microsoft and Deutsche Telekom ('DT') announced that Microsoft will offer Office 365, Azure and Dynamics CRM from 2 data centers in Germany under a model where DT will be the 'Data Trustee'.

- All German customer data only stored in Germany

- DT will have Exclusive control over Microsoft customer data, Microsoft will have no ability to access the data or physical access to the data center absent:
  - Permission from DT or
  - Permission from the customer

Microsoft’s Business Response (Part 2)

- Microsoft has also deployed an option in Office 365 and other products called ‘Lock Box’
- Lock Box requires authorizations from a customer’s authorized administrator before the customer’s data is made accessible to Microsoft employees in its cloud systems
- Per Microsoft:
  - the Lock Box code is ‘baked into’ the system and cannot be bypassed
  - Any request by a government for customer data can only be complied with if the *customer* agrees. Forcing the government to go to the customer directly for the data


slide to unlock
DIGITAL PANDORA'S BOX
FBI
NickANDERSON ©2.17.16 HEARST PAPERS

FBI v. Apple - Overview

- In 2014 Apple made a conscious choice to encrypt data on its iPhones such that not even Apple can decrypt the data
- The issue: to what extent can the US courts compel a manufacturer to assist the government in unlocking one of its products in response to a search warrant – where the data in strongly encrypted by design of the product itself
- In the absence of specific US legislation, the US government hung its hat on the All Writs Act (a law dating back to 1789)
- The San Bernardino California case is the most well known example of the assertion of the All Writs Act, but there have been at least 11 other cases in 2015 and 2016.

FBI v. Apple – Overview (con't)

- The basic facts of the San Bernardino case –
- Note: other than the data in the particular iPhone the FBI had already obtained:
  - From Apple, the data that was previously backed up to the iCloud from the phone
    - Apple encrypts data in the iCloud but holds the keys so it can decrypt and comply with government demands
  - From the telecom provider - the call records, SMS, tower location data and other metadata
  - The only data sought by the FBI was what was on the iPhone and not backed up to iCloud
- Key Question: In the absence of specific legislation can a court order (conscript) a company to develop code to effectively hack/compromise its own product to comply with a search warrant?

FBI v. Apple – Reaction….

- US legislation has been proposed that would require “"any person who provides a product or method to facilitate a communication or the processing or storage of data" to provide data in intelligible form or technical assistance in unlocking encrypted data and that any such person who distributes software or devices must ensure they are capable of complying with such an order”
- This legislation is not expected to pass anytime soon

U.S. v. Apple and Microsoft – The Perfect Storm

- A "perfect" outcome for the US –
  - A cloud provider is forced to compel its subsidiary to divulge its customer's email, and for either Congress to mandate that a "back door" be built into encrypted devices or for a US court to again order a tech company to write code to compromise its own product (and for that order to upheld on appeal)
- When taken together the US government's 'Nowhere to Hide' objective can distilled as follows:
  - *To be able to compel the disclosure of, hack into or otherwise access (via US legal process) data stored in the cloud or on a computer anywhere on the planet, and compel access to data stored on any device that US law enforcement has in its possession or control*

Global Implications –

- The fundamental issues raised in the Microsoft and Apple cases are also relevant in many other countries, but differences in law and politics may result in inconsistent outcomes and upset tech business models
- Russia has implemented an ‘Anti-Terrorism Law’ mandating that every provider must log all Russian Internet traffic for up to one year. Russian servers of a VPN “Private Internet Access” were seized without any due process. The law also requires telecoms and Internet providers to store the private communications of every customer for 6 months. This includes phone calls, texts, photos. Metadata must be stored 3 years. Whatsapp, Wickr and other encrypted messaging apps must hand over keys.
- The French government has pressed ahead with plans to punish tech companies who do not allow access to encrypted data
- The UK government has passed sweeping new laws allowing the government broader access and surveillance capabilities. David Cameron said there should be no digital place the government cannot reach
- Thailand’s laws already are broad enough to require a tech company to provide access or face fines/penalties as are Singapore and Malaysia’s
- The Chinese government is continuing to pressure US tech firms for access. A US win in the Microsoft case and/or the Apple cases will embolden China to pass similar legislation

Effect on Business Models

- *Uncertainty is the only certainty* at this point
- ***Recommended Strategy**: Make the Government have to go to the customer for the customer's data – but watch out for a government response similar to what has now been implemented in Russia*
- Build in strong encryption in the cloud and devices AND *put the encryption keys only in the hands of customers or trusted third parties*
- Imaginative approaches by both cloud and device manufacturers (e.g. the Data Trustee approach) are required to provide comfort to customers worldwide
- What happens in the US will continue to drive the global models
- This is not only about law enforcement lawful access – courts in civil cases *can also* order a provider to divulge customer data stored in clouds

A Few Words About Biometric Keys…

FBi ! OPEN THE DOOR, SiRi !
CHAPPATTE
International New York Times

Application and Key Takeaways –

- The US government's 'Nowhere to Hide' strategy and objectives are clear
- We cannot predict the ultimate outcome or success of the US government's approach or how other countries may react. Ultimately legislation is the likely outcome
- Business models for *cloud providers and device manufacturers* should optimally focus on
  - Empowering customers by providing them with the encryption keys with no back doors. Force any government seeking customer data *to contact the customer* (and not the cloud provider or device manufacturer)
  - Until the issue is finally resolved by the U.S. Supreme Court or Congress, consider legal structures for overseas subsidiaries to insulate the parent from a US lawful access demands (e.g. Microsoft data trustee structure)
  - Government/legislative lobbying efforts to influence the outcome of any potential legislation

Apply What You Have Learned Today

- Next Week:
  - Consider how the US ‘Nowhere to Hide’ strategy may impact your business
  - Initiate an evaluation of your company’s risk profile as it relates to lawful government access in each jurisdiction your company does business in
- Over the Next Four Weeks:
  - Complete the risk profile evaluation and develop risk mitigation strategies to shift the obligation of disclosure in response to legal process from your company to the customer. Empower the customer to deal with the demand
- Over the Next Three Months
  - Implement the risk mitigation strategies. Monitor the changes to the law and events and be prepared to re-visit the risk profiles and mitigation strategies given the dynamic and global nature of these issues.

QUESTIONS
ANSWERS

THANK YOU!

Jeffrey J. Blatt

Of Counsel

Tilleke & Gibbins International Ltd.
Bankgok, Thailand

E: jeffrey.b@tilleke.com

For more information please visit our website: www.tilleke.com