RSAConference2017
Singapore | 26–28 July | Marina Bay Sands

POWER OF OPPORTUNITY

SESSION ID: PGR-F04

In Tech We Trust: Securing Privacy in a Global Surveillance State

Jeffrey J. Blatt
Of Counsel
Tilleke & Gibbins International
Bangkok, Thailand
Twitter: @techlawexpert


1984
WAS
NOT
SUPPOSED
TO BE AN
INSTRUCTION
MANUAL

A little more about me…

- Pioneer Silicon Valley Tech/Telecom Lawyer (e.g. Apple, Intel, Broadcom)
- Key Member of Executive Team that built and launched Astro in Malaysia
- Board member of Sri Lanka Telecom (2008-2016): Chaired Risk Management Committee; Senior Tender Board. Drove cyber security initatives
- Experienced U.S. Law Enforcement Officer/active certification by Calif DOJ to participate in electronic interception/surveillance
- Accused of Being a Cloud Security and Privacy Evangelist:
  - One of first Tech Lawyers interviewed in US v. Apple case
  - Frequent speaker/author on cyber security, privacy/lawful gov't access

Our Objectives In This Session

- Explore the US Government's 'Nowhere To Hide' (N2H) strategy to reach data stored on any device in its possession; stored in any Cloud anywhere on earth; and remotely hack computers anywhere on the planet to identify users and obtain data using a US search warrant
- Discuss the global implications of the N2H strategy as adopted by the US and many other governments worldwide – a new 'Wild West' in Cyberspace
- Explore a New paradigm: tech companies stepping in as champions of privacy rights on the basis of business impact of N2H

Our Objectives In This Session (con't)

- Consider: are users entitled to a 'Digital Safe Space' free from government or third party access?
- Explore how the N2H strategy is disrupting service provider's global business models, local operations and customer expectations of privacy.
- Explore how tech business models are therefore being driven by the actions of the governments' lawful access demands
- Explore risk mitigation approaches for enterprises and users
- Consider potential future evolutionary paths depending on actions of tech and reactions of governments

But first.....

Tilleke & Gibbins

‘Nowhere to Hide Strategy’ (N2H)

‘Nowhere to Hide Strategy’ (N2H)

- The US government’s N2H strategy comprises three key elements. (Note: many other nations follow similar strategies):

  - First: Compel cloud service providers to provide access to customer data stored in servers anywhere in the world (U.S. v Microsoft/U.S. v Google cases)
    - *regardless of where the data sought is stored and notwithstanding local country law where the data is located*
      - Microsoft challenged a U.S. search warrant seeking access to customer emails stored in Dublin, Ireland. U.S. District court issued the warrant, and ruled in favor of the U.S.-- Microsoft then appealed to the Second Circuit. On July 14th 2016 a 3 judge panel of the Court of Appeals decided in FAVOR of Microsoft.

‘Nowhere to Hide Strategy’ (N2H)

- The US government lost at the 2nd Circuit Court of Appeals, but is seeking Supreme Court review *and*
  - The US convinced a US Magistrate in a similar case in the Eastern District of Pennsylvania that a US search warrant can compel Google to disclose data located outside the US under the Stored Communications Act

<u>Bottom Line</u>: The US is aggressively pursuing this first element of the N2H strategy – the gov’t is determined to be able to compel Cloud providers to disclose user/enterprise data no matter where on the planet the data is physically located

Global Implications of N2H First Element -

- A US Supreme Court decision in favor of the gov't (or the passage of new legislation) would dramatically change the risk profile for companies and individuals when deciding to put data in the cloud
- For example -a Thai company, using a cloud service provider based in Singapore for its corporate email, may find its emails are divulged to the US government without going through any legal process in Singapore (perhaps in violation of Singapore law) if the cloud provider has sufficient presence in the U.S.

N2H Second Element….Access to Any Digital Device

FBI v. Apple - Overview

- In 2014 Apple made a conscious business decision to encrypt data on its iOS devices such that not even Apple can decrypt the data
- Apple created a ‘digital safe space’ by corporate decision independent of any legal requirement to do so
- One issue is to what extent can governments compel a manufacturer to assist in unlocking one of its products in response to a search warrant – where the data in strongly encrypted by design of the product itself
- 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 15 other cases in 2015 and 2016 with over a thousand devices waiting to be decrypted for LE

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 in this case was what was on the iPhone and not backed up to iCloud
- Key Question: In the absence of specific ('back door') legislation can a court order (conscript) a company to develop code to effectively hack/compromise its own product to comply with a search warrant?
- Apple and much of the tech industry say 'no'/Gov't says 'yes'
- Government position: there are no 'digital safe spaces' – People cannot 'go dark'

N2H Third Element: Hack Computers to Get Data

N2H Third Element: Hack Computers to Get Data

In 2016 the FBI successfully lobbied to broaden Rule 41 of the US Federal Rules of Criminal Procedure

- A US judge can authorize 'Network Investigative Techniques' in a search warrant to remotely hack/gain access into any computer *anywhere in the world* in a US criminal investigation

- 'PlayPen Cases': FBI seized and ran dark web child porn website accessible via TOR, and deployed malware which downloaded when a person downloaded content – reporting the users actual IP address.
  - Hacked over 8000 computers/120 countries
  - Malware ('NIT') deployed worldwide in computers of users who attempted to download off Playpen - regardless of local laws
  - US search warrants issued *based on the IP addresses reported by the malware*
  - Subject's IP addresses reported to other nations' LE for prosecution in those countries

Third Element: Hack Computers to Get Data (con't)

- Since 'PlayPen' other nations are deploying malware globally in similar operations (e.g. Australia) for LE and intelligence purposes

- The Australian Federal Police (AFP) took over the child porn site 'The Love Zone' and ran it deploying malware catching 30 Americans in the process and turned the data over to the FBI for US prosecution. http://www.networkworld.com/article/3108412/security/aussie-cops-reportedly-hacked-us-tor-users-during-child-porn-probe.html
- Blurs the lines of where one nation's LE jurisdiction begins and ends in cyber space, resulting in multiple national authorities operating without regard to borders or treaties

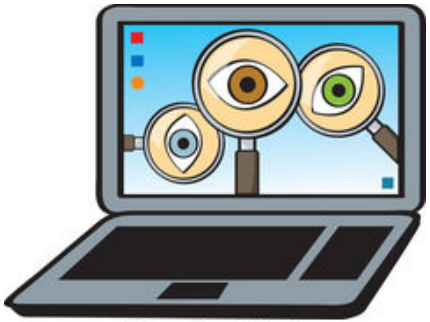
Third Element: Hack Computers to Get Data (con't)

- Let's Consider the Practical Effect of the Third Element :
  - LE agencies from around the world deploying malware on a planetary basis without regard to national borders or their jurisdiction for their own national purposes
  - Intel agencies from around the world are also deploying malware worldwide for their own objectives*, in addition to,*
  - Criminal organizations/non-state actors deploying malware and conducting cyber attacks
  - Search Warrants being issued based on the reported IP address
    - *Bottom Line: Cyberspace is further destabilized*

N2H 30,000 foot Quick Summary…

N2H 30,000 foot Quick Summary Review

- Prong 1: Gov’ts can access any data in any cloud regardless of the local laws where the servers are located (US v Microsoft, US v Google)
- Prong 2: Gov’ts can compel device manufacturers to require LE ability to access data in any device that the gov’t has physical possession of
- Prong 3: Gov’ts deploy malware to obtain data on devices not in their possession regardless of national borders
  - *Gov’t Objective: No ‘digital safe place’ – No way to ‘go dark’*



© Can Stock Photo

In Tech We Trust: Stepping into the Breach

- Rights of Privacy and Speech Historically arises from Constitutions, Bills of Rights and/or Legislation from the State:
  - Today many nations deny users the right of digital privacy, the right to 'go dark' and the right to a 'digital safe space' in the name of "national security" (e.g. UK, Thailand, Singapore, Russia, PRC, US)
  - *Some* Tech Companies are stepping in to provide users with rights that gov'ts seek to deny – and in the face of gov't resistance: Examples:
    - Apple device encryption
    - Microsoft's resistance to the US gov'ts extraterritorial search warrants
    - Encryption Apps (WhatsApp, Wickr, Signal) provide privacy globally regardless of local laws
    - Secure Cloud Service (Sync, Tresorit) alternatives to Dropbox where users hold encryption keys
    - Facebook (sometimes) in refusing to remove content that is 'objectionable' under local law (e.g. Thailand)
    - Twitter (sometimes) in providing a platform for discussion in the face of some gov'ts strict control of the media

Unprecedented in History…

- Tech Companies have stepped in to provide users with a 'digital safe space' regardless of local law and/or gov't resistance (when it's consistent with the tech company's business model)
  - This is unprecedented in history and game changing for users

BUT

- Govt's are powerful and are pushing back….with legislation and the power of arrest, prosecution and fines, for example:
  - Legislation requiring 'back doors' or other access to encrypted apps and devices
  - Potential legislation to require all data in a digital device (i.e. phone) be backed up to the Cloud with service or device provider holding the keys
  - Outlawing or blocking certain encrypted messaging apps or social media
  - Requiring all local user data to be stored in country

Cat/Mouse Opportunities for Tech

- Encryption technology controlled by end users (humans or enterprises) still provides the best overall protection from gov't surveillance and compelled access

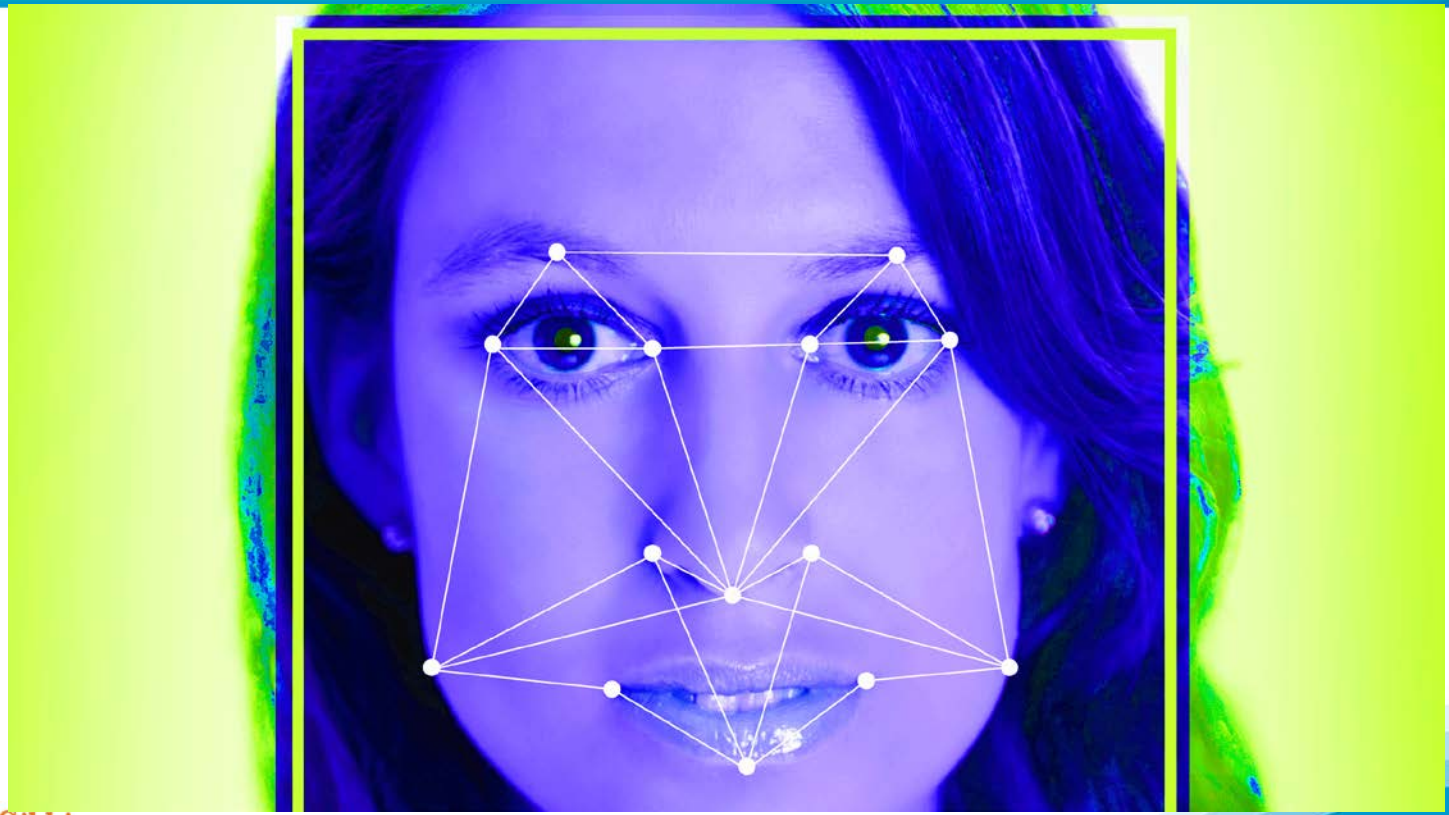
- A key issue in many situations is that for user data held by a third party provider, a gov't demand will include 'gag orders' preventing the service provider from advising the end user his/her/its data has been disclosed to the gov't

- *Tech Opportunities Include*:
  - Empower end users to create/control encryption keys for cloud and device based data
  - Create software to address gov't NIT/Malware and preserve anonymity on the Web
  - Create enhanced built in VPNs to ensure that POPs are outside the jurisdiction where the user is currently (no logging obligations)

Effect on Business Models

- *Uncertainty is STILL the only certainty* at this point
- ***Recommended Global Strategy for Tech Sol'ns***: *Make a 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, the UK and elsewhere*
- Build in strong encryption in the cloud and devices AND *put the encryption keys only in the hands of customers*
- Imaginative tech and business approaches by both cloud and device manufacturers to require a Gov't to go directly to the user for data (e.g. a Data Trustee approach)
- 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

Quick Aside: Biometric Keys…Security vs Privacy



Application and Key Takeaways –

- The US government's 'Nowhere to Hide' strategy and objective is clear and is being followed by many nations. It is not just a US issue
- Tech companies are uniquely situated to provide users with digital privacy otherwise denied by governments and/or national law
- This is a Cat and Mouse Game – *it's all about leverage (tech v gov'ts)*
- 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)
  - Consider legal structures for overseas subsidiaries to insulate the local entity from a gov't lawful access demand (e.g. Microsoft data trustee structure)
  - Develop new software/apps to counter each of the three elements of the N2H strategy

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.

Tilleke & Gibbins

THANK YOU!

Jeffrey J. Blatt
Of Counsel

Tilleke & Gibbins International Ltd.
Bankgok, Thailand

E: jeffrey.b@tilleke.com