Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

Protecting corporate intellectual property: Legal and technical approaches

Michael G. Crowley *, Michael N. Johnstone

Security Research Institute, Edith Cowan University, 270 Joondalup Drive, Joondalup, Western Australia 6027, Australia

KEYWORDS
Law;
Privacy;
Security;
Encryption;
Cloud services

Abstract The recent FBI v. Apple case has the potential to turn a 227-year-old statute law into a tool for government agencies to gain access to personal and corporate information. Recent events such as 'Petraeus-gate,' hacked nude celebrity photos in the cloud, and the use of a search and seizure warrant in the United States seeking customer email contents on an extraterritorial server raise important issues for the supposedly safe storage of data on the World Wide Web. Not only may there be nowhere to hide in cyberspace but nothing in cyberspace may be private. This article explores the legal and technical issues raised by these matters, with emphasis on the court decision *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* and the subsequent upholding of that decision.

1. The tension between privacy and disclosure

The ease of use of the internet for business communication has been a boon in terms of keeping abreast of the market and collaborating with colleagues separated by geography and time zone. This ease of use, however, has fostered an attitude of complacency which exposes the information stored by users to greater risks of theft in a highly competitive business environment.

The impetus for protection of data lies in personal privacy and business concerns generated by the revelations of WikiLeaks, Edward Snowden (Sifry, 2011), and business reality. For the latter, cyberattacks are one of the biggest threats facing businesses. The cost of data breaches at companies is expected to hit $2.1 trillion globally by 2019 (Kharpal, 2015). Maintaining confidentiality of data in this environment has become a necessity for businesses and individuals seeking to take commercial advantage of their newly-developed knowledge, skills, and information.

In the ASEAN region, cybercrime is recognized as one of the eight transnational crimes, in addition to illicit drug trafficking, money laundering, terrorism, arms smuggling, trafficking in person, sea piracy,

* Corresponding author
E-mail addresses: m.crowley@ecu.edu.au (M.G. Crowley), m.johnstone@ecu.edu.au (M.N. Johnstone)

and international economic crime. The addition of cybercrime to the list was decided in the Official Senior Meeting on Transnational Crime (SOMTC) which was held in Singapore on October 10, 2001. Cross-national variations can encourage what is referred to as 'regulatory arbitrage,' with individuals and groups committing offenses in territories where they are assured of facing little or nothing in the way of criminal sanctions. The jurisdictional problem governing cybercrimes has caused the legal authority of each country to act like an athlete who runs around a track in a stadium while the cyber criminals are the peers and spectators, analyzing the way the authority runs and determining the leaks and weaknesses. No matter how many laps around the track the authority runs, the outcome is always the same: to arrive at the finishing line just to discover that it is the starting point all over again (Rahman, 2012). However, recent events in the U.S. indicate governmental concern about a lack of asset protection may be turning as government agencies find they can no longer eavesdrop into and/or covertly access certain databases and equipment.

Potentially embarrassing photos stored in the cloud (Stuart, 2014) have been the subject of a successful targeted hack despite assumed secure storage (Rushe, 2014). The Petraeus-gate and nude photo matters highlight some underlying risks associated with internet use; data are not necessarily confidential, which has implications for the security of corporate intellectual property. Regrettably, these cases—whilst perhaps sensational (and thus particularly visible)—are not isolated. The BBC (2009) reported on 13 instances of data loss of medical records, prisoner records, and defense personnel records between 2007—2009. Whilst these cases appear to be ancient history, recent events such as the aforementioned one suggest the problem still exists. The web is also an increasingly valuable source of information for security agencies driven by the realization that traditional jurisdictional limitations may not apply to data on the web, as the nature of electronic data allows existing legal tools to defeat anonymity and confidentiality. Governments also recognize the activities of non-state actors (businesses and other parties) in cyberspace. For example, "In addition to the actions of countries, non-state actors have the growing ability to adversely impact the global commons through activity. . .[through] the use of readily available and highly disruptive technology including cyber capabilities" (Australian Government Department of Defence, 2016). The recent decision *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 13 Mag. 2814 (hereafter referred to as the Microsoft E-Mail case) highlights a new jurisdictional paradigm. While Petraeus-gate demonstrated that even determined attempts at confidentiality can be overcome by security agencies, in the Microsoft E-Mail case the judge issued a search warrant requiring Microsoft in the U.S. to produce information stored in Ireland. An appeal confirmed this decision. However, on July 14, 2016, a three-judge panel of the United States Court of Appeals for the Second Circuit ruled unanimously in favor of Microsoft. The court held that American legislation did not extend to the seizure of customer email content held exclusively on foreign servers. Still being entertained by the court, however, is the FBI demand that Apple unlock the encrypted contents of a phone owned by one of its customers (*In the Matter of the Search of an Apple IPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, United States District Court for the Central District of California No. ED 15-0451M, hereafter FBI v. Apple case). This article explores this mélange of law, technology, and security and provides some words of wisdom to a hypothetical sunshine entity seeking to protect and profit from recently-developed, high-value intellectual property.

2. Legal approaches

2.1. The Microsoft case

The decisions in the Microsoft E-Mail case and subsequent appeal raise important legal issues. Petraeus-gate demonstrated the ability of security agencies, acting lawfully, to piece together fragments of electronic data to find a source. The nude photos hack demonstrated that advertised security measures may not be much help against a determined hacker, possibly raising private legal remedies. What is clear from these three matters is that what was once private is now no longer private if linked to the internet. While determining jurisdictional limitations was a key issue in the Microsoft E-Mail case decision, other factors worth considering also arose. This was one of the very few cases that made it into the public arena, as service of such warrants generally imposes limitations on those served (e.g., Zetter, 2013). Without assessing the contents of such warrants and the data handed over it is not possible to ascertain whether or not the warrants achieved a national security purpose.

The nude photo hack ignores jurisdictional limitations because of the nature of hacking. Jurisdictional limitations usually apply to the execution of a