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

search and seizure warrant and that is what makes the Microsoft E-Mail case important. A hypothetical web user always faces the risk that determined security agencies acting legally might access their internet data. The nude photos hack tells this same user that commercial security measures may not be adequate. The Microsoft E-Mail case tells our user the data may not be safe no matter where they are stored.

Jurisdiction is generally state-based so that a legal instrument issued in the U.S. is limited to its own territory. Each state has resorted to the use of Mutual Legal Assistance Treaties (MLAT). These treaties provide an agreed process for service and execution of warrants seeking information from outside the jurisdiction. However, the state in which the warrant is served may decline the request. The decision in the Microsoft E-Mail case stepped around these international treaties because the warrant was served within the U.S. The essence of the judgement is that Microsoft is to deliver email content held on one of its servers in Ireland to a New York Court because the warrant was served to Microsoft in the U.S. Microsoft opposed the warrant because the email content was held in Ireland, while the government argued the warrant required Microsoft to hand over email content no matter where it was held. At first blush this may not seem unreasonable until it is recognized that the impact of the judgement means all internet and cloud companies operating out of the U.S. may be required by the government to hand over content stored in other jurisdictions.

Judge Francis's decision turned on the nature of digital information and the impact of a search warrant. In this case, Microsoft held non-content information, address, and basic related details about the email account in the U.S. but the crucial email content was held on its server in Ireland. The search warrant required Microsoft to hand the email content over to the U.S. court or breach U.S. law (i.e., Carroll, 2014). In complying, Microsoft may or may not breach Irish law but would almost certainly breach European Union data transfer laws.

Additionally, this warrant is jointly covered by various U.S. laws, including section 108 of the Patriot Act. In particular, emphasis was placed on the meaning of the words "where the property is located" being the location of the ISP, not the location of any server. It means the restrictions governments face with physical searches of a property do not apply in an online environment, rather the use of this particular warrant shifts the onus on production to Microsoft. This is because the warrant is a combination of a search warrant as usually used in criminal proceedings and a subpoena, a writ requiring persons or things to be delivered to the court. Our hypothetical web user would, as a general rule, become aware that personal data had been seized, either because the service provider may have told the user or the data would have appeared in open court proceedings. The nature of these warrants preclude the former because the public cannot rely on court proceedings concerned with national security issues being public.

Any assumptions by web users that data are secure and private is meaningless. Stevens (2009) has blogged on the fallacy that if you have nothing to hide you have nothing to fear. In the Microsoft E-Mail case the nature, size, and reach of Microsoft now poses privacy problems for our hypothetical web user. Microsoft Corporation is an international company headquartered in the U.S. While Microsoft is generally recognized as a major software developer, it also operates a significant internet service including email services and data storage. In 2011 Microsoft purchased Skype. Importantly for the purposes of this article Microsoft has office locations in some 211 countries. Microsoft (2016) also has a privacy statement but this may be rendered useless by the Microsoft E-Mail case.

It is Microsoft's activities in cyberspace that are at the center of the Microsoft E-Mail case. While cyberspace may be a construct in the ether it has terrestrial accoutrement such as data storage, chat rooms, files, and online shops. Users have a digital footprint that can transcend borders. This borderless nature can mean the host of your email account may be on the other side of the world. This case involved the U.S. and the Republic of Ireland. When the source or location of internet data is involved in litigation, whether civil or criminal, courts have to decide what conduct is relevant and where it occurred. Historically, (i.e., *Airways Corporation of NZ Ltd v. PricewaterhouseCoopers Legal* [2002] NSWSC 138) the focus was on where the damage was inflicted. In another decision (*Dow Jones v. Gutnick* [2002] 210 CLR 575, p. 87), observations were made about "special difficulties for the legal regulation of its content and, specifically, for the exclusion of access in defined jurisdictions." These legal decisions accepted the general principle that Australian law was meant for Australia. In Verizon Communications Inc.'s motion to participate as *amicus curiae* (friend of the court) in Microsoft's appeal against the decision in the Microsoft E-Mail case, Vatis and Novack (2014) cite Morrison v. National Australia Bank Ltd., 561 US 247, 248 and stated the court should remember the "longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States."

What Judge Francis did in the Microsoft E-Mail case gave greater weight to the necessities of law enforcement over those traditional concerns of jurisdiction and privacy. Judge Francis considered the domestic and international legal expectations about access to internet data. Because the U.S. has a strong legal tradition and an overarching constitution, security agencies either conduct covert, and probably illegal, surveillance or seek to use pre-existing legal remedies. The recently published Australian Law Reform Commission (2014, p. 17) report observes that invasions of digital privacy occur with ''increasing ease and frequency'' and ''personal information, once put online seems impossible to destroy or forget.'' The report went on to note that while Australian laws offer protections there is ''significant inconsistency in the law between jurisdictions'' (p. 26). These inconsistencies were overcome by recommending federal legislation to ensure consistency across Australia. Additionally, the report recognized the potential impact of surveillance on important freedoms. It quoted Professor Neil Richards, who said ''it can chill the exercise of our civil liberties,'' causing people to ''self-adjust their behavior even if they are not doing anything wrong'' (p. 281).

2.2. The FBI v. Apple case

While the Microsoft E-Mail Case exposes cloud users, email and data storage entities linked to the U.S. to possible future access by U.S. government entities, the FBI v. Apple case could turn a 227-year-old statute into a stunning new tool for government agencies seeking access to personal data. The use of the All Writs Act (28 U.S.C.§ 1651) raises the intellectual property stakes for those entities relying upon innovation, encryption, and technical advances to maximize market opportunities. Historically, the All Writs Act has been a favored tool for removing state cases to federal jurisdiction (Hoffman, 1999; Steinman, 2000). However, in this case, Apple has become the 'party of necessity' rather than the 'jurisdiction of necessity' (e.g., Steinman, 2000) because the FBI wants access to the contents of one of Apple's smartphones. There is some precedence for such orders using the All Writs Act. In *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), a majority of the U.S. Supreme Court held that the All Writs Act provided grounds for the federal court to force a non-party into current proceedings if that party is ''in a position to frustrate the implementation of a court order or the proper administration of justice.'' In *New York Telephone* the company was the only entity/party capable of giving effect to the court's order that pen registers be installed on two telephone lines so the FBI could capture telephone signals without being detected (Hoffman, 1999; Steinman, 2000). Apple's case deals with the not-unreasonable belief that only Apple has the knowledge and technical capacity to open access to the target iPhone 5C used by Syed Farook, who along with his partner killed 14 people and injured 22 others in San Bernardino, California on December 2, 2015. Syed and his partner were subsequently killed by police but Syed's smartphone may have data that could assist police in identifying any communications with Islamic State and other militant groups (Reuters, 2016). The problems for the police are many. For example, the iPhone 5C has strong encryption with an auto-wipe password function and Syed stopped automatic backups about six weeks before the shootings (Hollister & Guglielmo, 2016). While Apple has cooperated in providing access to Farook's iCloud data, it has drawn the line at providing what would in effect become a 'master key' for Apple's smartphone.

In the ongoing legal proceedings between the FBI and Apple, the FBI is attempting to use the All Writs Act (1789) to get Apple to change its software (Hollister & Guglielmo, 2016). As Hollister and Guglielmo (2016) noted, a statute signed into law by George Washington using a quill and ink is being used to force access into a smartphone database. This case shines a very bright light on two competing claims: the need for a business to protect an asset and the perceived need by a government to have access to that asset. There is a necessary balance between protection of intellectual property and using that property for profit, and a technology company's reputation. No one will know what you have developed if you do not tell anybody and you do not store it on the internet, but once you have something special it is only a matter of time before someone copies, steals, or works out how you did it. Added to these risks is the threat of law enforcement agencies seeking access to what could be called the holy grail of your business—the intellectual property that underpins a key business advantage. In Apple's case, customer privacy is now fundamental, with Apple CEO Tim Cook (2016) saying the fight is about security and privacy for everyone, and attempts by the FBI to use a 227-year-old law to comprise its most important products sets a ''dangerous precedent.'' In his message to Apple customers, Cook wrote, ''The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers.'' He added:

> Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security

> features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software —which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.
>
> The FBI may use different words to describe this tool, but make no mistake: building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

Apple cannot ignore any court order to provide access but to do so without contesting could result in serious customer dissatisfaction. Apple has not ignored the lessons from WikiLeaks, Snowden, Ashley Madison, and published cyberattacks—some involving industrial espionage—but it risks losing control over intellectual property and a loss of profit. In achieving a comprise between the two extremes, the sunshine entity needs to take account of recent technical and legal issues if it is to succeed in taking advantage of its new discovery. At the core of any data protection lies encryption. While the historical diplomatic pouch allowed diplomats in foreign lands to physically send data home knowing other states would respect the tradition that the contents were sacrosanct, prudence would require certain contents were nonetheless encrypted. Pouches can be lost or stolen, planes crash, and there is always the risk temptation will overcome tradition. With the development of the internet it is possible to maintain confidentiality over transmitted messages so long as the key to the encryption remains secret. However, total reliance upon encryption may also give false security. As the American computer security expert, Jon Callas, noted: encryption is not going to solve traffic analysis collected as metadata especially as "a lot of the metadata that they [the authorities] are interested in is extraordinarily hard to protect, and in most cases you may not be able to protect it" (Mansfield-Devine, 2013, p. 19).

3. Technical approaches

The aims of information security are confidentiality, integrity, and availability. The former is important in terms of providing security for data assets that represent intellectual property. Conventionally, confidentiality is preserved in the digital world by some kind of encryption system that is very difficult (but not impossible) to break. The potential loss of IP is exacerbated by the use of cloud computing by many firms. The business driver for cloud services is clear—to reduce costs—but this shifts the locus of control with respect to security, leading to potentially unexpected outcomes with respect to IP. Nonetheless, cloud services remain popular so it is useful to examine how security can be preserved in a cloud environment. In such cases where trust is an issue, encryption is fundamental to any storage of data.

There are many ways data can be protected to maintain confidentiality. Businesses working at the cutting edge of technological advances need to ensure their data/research/discoveries are not accidentally exposed or stolen by a competitor. Common sense requires a three-step process. The first step involves using equipment that is not connected to the internet or accessible from external sources; some firms do this. The second step means limiting access to the protected space to trusted persons who are not permitted to transport USB keys or similar devices into the area. In some agencies, bringing writable media into a secure space is grounds for immediate termination. Finally, there is a need for encryption as a last resort. Once a product moves to the production/distribution stage encryption may be the only measure protecting valuable intellectual property. In this section we examine the principles and practical aspects of encryption and then look at cloud services and metadata as complicating factors.

3.1. Encryption

Schneier (1996, p. xix) stated, "It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics." Some five years later his views had changed somewhat: "It's just not true. Cryptography can't do any of that" (Schneier, 2000, p. ix). Nonetheless, it is instructive to examine precisely what encryption can do to preserve privacy.

Encryption requires keys, which raises the question: "Who has the key to decrypt our IP?" Many cloud providers use shared-key encryption, so your data is (or rather, may be) safe in the cloud—but not from them. The terms of service from cloud providers are of interest here. Google gives its automated services permission to access data on its servers. Microsoft allows employees to view files on its servers. Dropbox allows its employees and trusted (unspecified) third parties to view and share files on its servers. All of these providers might have valid reasons for needing to access a firm's data (= IP), but data leakage for the purposes of corporate espionage should not be one of them. How can providers be protected so that they do not inadver-

tently share another firm's data? Zero-knowledge cloud storage is touted as an answer.

The concept of zero-knowledge systems is not new (Bellovin & Merritt, 1992). The idea that a user could prove to another party that he/she knows a password without having to reveal that password is attractive as the password is never transmitted and thus cannot be captured by a third party 'listening in' on the conversation.

Zero-knowledge cloud storage means that a client (the IP owner) encrypts the data before it is uploaded to the cloud. That way only the client has the key. The encryption is usually performed with software provided by the cloud service provider. There is a certain level of trust inherent in the use of such a system. A client assumes (or trusts) that the software does exactly what it supposed to do, does not contain any defects that render it open to attack by third parties, and does nothing else. Much like zero-knowledge systems, the concept of backdoors into systems has been extant for some time.

If a client cannot (or chooses not to) trust a cloud provider, the next option is for the client to encrypt the data before it is uploaded to the cloud, but with open source encryption software selected by the client. At this point the client has control over the key(s) and is now not concerned by any agreements between cloud providers and their third parties, trusted or not. Of course, if the client now wishes to perform any operation (read, update, append, write, etc.) on the stored data, those data must be decrypted. In the decrypted state data may be open to theft. This is not entirely true as homomorphic encryption provides a way to perform a limited subset of operations on encrypted data without decryption at any time.

Usually, data are encrypted at the source and decrypted at the destination. This is often achieved with asymmetric encryption, where two keys are needed. The first is a private key which is held securely by the destination and the second is a public key which is published widely and thus made available to anyone (the aforementioned source) who wishes to send an encrypted message to the destination. If the keys are large enough, it will take a long time (months or years) for the encryption to be broken by a third party. Given that information has a time value, this is often considered a realistic trade-off. The keys have the useful property that a message encoded with one of the pair can only be decoded with the other key and vice versa. So, if Bob wishes to send a message (say an email) to Alice, he looks up her public key and encrypts his message with that key. Only the secret second key (held safely by Alice) can decrypt the message, thus assuring confidentiality. A useful side-effect of this process is that it provides a method for digitally signing communications and/or documents. Assuming Bob also has a set of public and private keys, he can encode a message first with his secret key and then encode this already-encoded message with Alice's public key. This doubly-encoded message can now be sent to Alice. Notice that when Alice decrypts the message with her secret key (as only she can) the result is still encoded by Bob's private key. The only key that can now recover the message is Bob's public key (to which Alice or anyone else has access), thus proving that the message could only have come from Bob.

There are some difficulties with using this system. The keys must be related to large prime numbers to assure the mathematical properties of the encryption and decryption functions. It takes time to find relatively large prime numbers. By large, we mean hundreds of decimal digits. It is evident by a simple check that 11 is a prime number, however, consider a somewhat larger number such as $2^{57,885,161}$-1 (a number with over 17 million digits). It takes some time to ascertain that this number has no factors apart from 1 and itself. Kleinjung et al. (2010) report being able to determine the primes within a 768-bit (232 digit) number using several hundred computers over two years. The only reason that a third party who is not Alice cannot decrypt Bob's message is that finding the factors of a very large number takes a long time. Gribbin (2013) estimated that finding the factors of a 1024 bit (300 digit) number is computationally infeasible on a conventional computer. It also takes time to encrypt and decrypt messages. Ultimately, the users must decide the value of the trade-off between time/security and convenience. Even if data can be secured by encryption, this may not assist if a user is forced by a court to produce his/her secret key, a matter we will discuss in the next section.

3.2. Cloud services

Mell and Grance (2011, p. 2) define 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 provisioned and released with minimal management effort or service provider interaction." It encompasses more than storage, which is perhaps the most conventional view of cloud services. Different types of resources, such as network bandwidth or servers (physical or virtual machines), can be hired for any length of time, which is an approach that is more flexible than simply hiring disk space.

The driver for cloud computing is, of course, cost. Market forces determine the price of the services on offer, thus providing cost-effective services to customers, without the need for highly-educated on-site personnel required to maintain expensive equipment. This section considers the risks to security and privacy in employing cloud services.

Cloud service vendors claim that costs are lower than conventional models of IT service provision, as low as 12 cents per Gb of storage per month (RackSpace, personal communication, August 2014). Mason (2011) presents a contrasting view and asserts that a more traditional model of data storage is more cost effective. However, minimizing cost, whilst laudable, should not be the sole objective. Security of intellectual property and the need to keep valuable business data private are also key objectives for most firms, should they wish to maintain their hard-won market share. The case of the MineLab metal detectors (Fowler & Cronau, 2013), where the firm concerned found that its product had been copied and was being sold without its knowledge, serves as a reminder of the seriousness of the problem.

The need for security and privacy is made more difficult as noted by Shostack and Stewart (2008, p. 89), who claim that most software is insecure: ''Because security is difficult for prospective customers to evaluate, it is rarely prioritized above other factors in their purchasing process.'' This would likely be multiplied as the environment in which the software operates (e.g., cloud computing) becomes more complex. Johnstone (2009) notes that the lack of security in software is due to the tension between function (as seen by a customer) and security (which is often invisible). As software is ubiquitous, this reliance on software that may be insecure raises concerns in terms of business continuity, never mind privacy.

As previously mentioned, confidentiality, integrity, and availability are considered the core principles of information security. There are several aspects of these principles that are worth bearing in mind with respect to cloud computing. Confidentiality in a cloud-based system is maintained in two ways; first, a user of cloud services does not know which physical location stores the data and second, the data may be split into several parts across several locations. Thus the appearance of a single file as a user view is preserved by the cloud facade as part of 'software as a service.' In contrast, the notion of preserving integrity appears to be at odds with the same benefits which assure confidentiality (i.e., the separation of the file into several parts across multiple locations). The platform layer is responsible for collecting the parts of the file and arranging them into a coherent (and correct) whole—a service which is (and certainly should be) transparent to a customer of the cloud service. Availability is handled by the infrastructure layer.

This describes the scenario where all of the cloud service layers function flawlessly to provide the expected (paid-for) services. How would attacks on confidentiality, integrity, and availability affect the provision of cloud services? A conventional attack on availability is denial-of-service (DoS). A DoS attack on a cloud service provider will almost certainly result in a loss of availability. A less obvious outcome is that a DoS attack may also affect integrity if a file is partially constructed. A partial file may be of no value to a customer as not all file types are sequential. There may also be an opportunity for data to be modified or leaked (a breach of confidentiality) because of a failure in the other service provision layers.

These issues are further complicated because the attacks can be launched by a variety of individuals or interest groups from disgruntled employees (more conventional) to lone hackers, activist groups, business competitors, and nation states. Most of the software needed for these attacks is freely available, thus the attacks pose significant business risks. This suggests businesses need the freedom to protect their information assets from others with appropriate security and privacy measures if they wish to remain competitive and have control over their established intellectual property.

The metadata retention proposal by the Australian Government (Bergin, 2014), whilst viewed with dismay by telecommunications providers (due to the apparent cost of retention, not for any concerns by the providers regarding customer privacy), is interesting because the providers were already storing said metadata; the government was asking for a slightly longer retention period. The claim that Microsoft read the email of one of its Hotmail customers for its own purposes certainly muddies the waters (Hern, 2014) and the Preska decision (No. 13 Mag. 2814, M9-150) against Microsoft has not increased business confidence in technology, especially cloud-based services that are outside of a firm's locus of control—especially given that many email and cloud providers host services physically on the west coast of the U.S. For example, the providers of Hotmail and Gmail (Microsoft and Google, respectively) operate data centers around the world, but most of these data centers are based in the continental U.S.

How then, may firms operate in cyberspace whilst preserving privacy and ensuring that security is maintained? Assuming that no data will travel through a satellite office within the jurisdiction of

the U.S., the obvious option is a cryptographic method where encrypting is easy but decrypting without the appropriate key is computationally very difficult. As mentioned previously, confidentiality, integrity, and availability are the core tenets of information security. The metadata retention proposal and the action by Microsoft present two different problems: one of tracking where someone has been (potentially an attack on privacy), and another an attack on confidentiality. Metadata retention is perhaps less of a problem for businesses as this may show what website was visited by an employee but not what he did whilst there. This leaves the latter, more serious problem of assuring confidentiality.

4. Discussion

Even with good asset protection things can go wrong. Not so long ago at Florida International University (FIU) in their new research and teaching laboratories on cybersecurity, including the Advanced Wireless and Security Lab (ADWISE) and the Cyber-Physical Systems Security Lab (CSL), something unexpected went wrong. For his class project, Andrew De La Rosa—a student in an ethical hacking class—decided to attack Bluetooth, a technology standard used to exchange data over short distances. He wanted to show that weaknesses in Bluetooth could allow him to download someone's private contacts. He picked a device at random on the FIU campus and hacked into it. ''When I ran the serial number, I saw it was registered to campus police,'' De La Rosa said. He rushed to the police substation at the FIU Engineering Center to explain. ''You're lucky you told me,'' the officer told him. ''Even if you're doing this for a class, I could have arrested you.'' Florida punishes unauthorized access to a computer system as a felony (Gretch, 2015).

In another related example, Dutch undercover investigative journalist Alberto Stegeman aired a program on the court security in Utrecht. He used a smartcard issued to one of the building's former staff to enter the court while carrying a fake gun. The same principle applies in the online environment. Many organizations are now aware of the gaps which can arise in their security, both at the physical and logical levels (Doswell, 2015).

The recent phenomenon of outsourcing of jobs to countries such as Mexico, India, Pakistan, and China has been controversial. Many of the lost jobs are the 'back office' tasks, handling copious amounts of sensitive information including Social Security numbers, credit records, medical records, and other financial information. Whilst in many Western countries there are federal and state laws that address the issues of information privacy, confidentiality, and the abuse of such data, the internet is not bound by international borders and therefore these laws have limited influence in foreign countries. These concerns were realized in October 2003 when a disgruntled Pakistani medical transcriber posted the medical records of several patients at the University of California, San Francisco (UCSF) to the internet. Upset at the lack of payment for her services, the transcriber sought to force the issue by compromising the information. The incident revealed that information sent offshore is prone to breach of confidentiality, that the obligations of those responsible for the integrity of the information are not well defined, and that consumers are not well informed of the potential problems or actual incidents. The subjects of computer security and related law enforcement in India and Pakistan have been called into question, but the same issues can arise in other countries where work is likely to be outsourced and the subjects of computer security and law enforcement are equally questionable (Lum, 2004).

4.1. Can the law make you do something?

In both the Microsoft E-Mail and the FBI v. Apple cases, government entities are using court procedures to make a company do something it does not want to do. What makes both of these cases important is that neither Microsoft nor Apple has broken the law. They are merely the gateways to data. In Microsoft's case it is also arguable Microsoft has obeyed international laws that the U.S. has upheld to date. Apple has taken steps to comply with the government, warning lack of adequate privacy protections aids criminal behavior. In both cases complying with the court orders has significant privacy impacts on customers and resultant reputational damage that could seriously impact profits. However, in both cases the impetus for compliance lies in countering criminal behavior.

The Apple case raises another issue. Can the court order someone, including a company, to do something that it may not be able to do? It seems from the information available Apple can possibly, with enough time and intellectual grunt, bypass its iPhone inbuilt security measures. Should Apple achieve this the government would be privy to the 'how'—providing a model for defeating future mobile phone security measures—probably rendering all mobile phones 'open access.'

What happens if Apple cannot defeat its iPhone security measures? The first problem will be: ''How will we know they cannot do it?'' What will be the test, the benchmark that would satisfy a court that, despite its order, Apple cannot do it—despite its

best efforts? To test any assertion by Apple that it could not breach its iPhone security would probably expert evidence in court, opening the prospect of commercial-in-confidence evidence becoming public regardless of any court orders to the contrary.

Davidson (2009, p. 18) argues that the rules needed for cyberspace cannot be based upon the rule of law notwithstanding the parallels; this is because the "rule of cyberspace is the natural, emergent order arising from data chaos." Information in cyberspace has different values to different people with cyberspace providing freedom and order for users. Davidson believes any attempt to control cyberspace will fail because of the special ability of cyberspace.

Microsoft's failure to date in its challenge of the warrant poses serious risks to individual privacy and serious commercial risks for Microsoft. Whether or not Microsoft wins, U.S. security agencies have forced businesses to review security and privacy arrangements. Carroll (2014) has reported that the German government told Microsoft it will shun data storage from U.S. companies unless the ruling is overturned. Foreign users and domestic Americans may well join the Germans and stop using U.S. internet services, a move that could adversely impact profit margins. Of more direct concern for American users is that other states may adopt the same tactics, including use of similar warrants served on Microsoft in their jurisdiction requiring Microsoft to hand over details of Americans stored in the U.S.

When you add the features of the Apple case to the mélange of law, technology, and security surrounding so-called 'safe' storage and assumptions by our hypothetical web user, nothing seems really secure. If the Microsoft E-Mail case had not made the news, had Microsoft not challenged but rather complied with the warrant, email users would be none the wiser that their email content stored outside of the U.S could be easily accessed without their knowledge by U.S. security agencies.

4.2. Is anywhere, any method of storage safe?

Given the scenarios described above, is the only safe computer one that is not connected to the internet (and is turned off and stored in a locked safe)? Unfortunately, it depends. Before answering the question, the pertinent sub-questions to ask are: From whom must the data be protected and for how long? This will depend on the nature of the data and who has control over it.

Inexpensive General Purpose computing on Graphics Processing Unit (GPGPU) cards can be clustered, capable of cracking a six-character password in seconds and a random 15-character password within a week. Such GPGPU systems can be built for $1,500 —not out of the reach of serious hobbyist users—therefore large random passwords are to some extent the way forward. Given that most people don't remember such passwords this has nurtured a growing industry in biometric identification systems which use some recordable, repeatable physical property of a person, such as a fingerprint.

For the user whose data must be kept secure and private for legal reasons (e.g., medical records), the answer possibly lies in homomorphic encryption schemes. Usually when encrypted data needs to be processed it must first be decrypted, then processed, and then finally re-encrypted. This could lead to a potential breach of confidentiality as remnants of the unencrypted data may be stored in an insecure place (e.g., a temporary file on a local computer). Homomorphic encryption offers a way to be able to process data in its encrypted form without the need for decryption, thus keeping confidentiality.

Ultimately, in the security chain, it is the human element that is the weakest link. WikiLeaks and the Snowden case (Sifry, 2011) provide convincing evidence towards this claim. Strong encryption is useless if the password is written on a Post-It note stuck to a user's monitor screen. Similarly, a large private key stored on a computer accessible via the internet is a breach waiting to occur. Finally, assuming successful encryption, the holder of the key may become a 'person of necessity' placed in the position of Apple with a court order seeking disclosure of the key. In 2007 the United Kingdom activated a clause in The Regulation of Investigatory Powers Act (RIPA) that allows a court to order a person to reveal a decryption key. Failure to comply carries up to five years in prison (Pinsent Masons, 2007). However, a court in Vermont has, in applying the Fifth Amendment, ruled a man cannot be forced to divulge an encryption key (McCullagh, 2007). There was a similar case in Atlanta where the accused had talked to her ex-husband and co-defendant in prison, whilst in Vermont the accused had only spoken to law enforcement agents and claimed the right against self-incrimination (Fakhoury, 2012). The rule in the United States is 'silence is golden.'

In the end it may well come down to whom and what can be believed. For example, what will happen should the suspect hand over the encryption key and what is subsequently found amounts to nothing of any significance? The Microsoft E-Mail case and the FBI v. Apple case might at first blush seem a clever use of law and legal process, but in the arms

race to protect privacy some citizens will take steps to protect their privacy. For example, a suspect may be prepared to reveal the sought-after encryption key because unbeknown to anybody else that same key has timely, instrumental, and/or jurisdictional defenses that need to be complied with to fully access all the data. Can democracies effectively legislate to stop mobile phone manufacturers producing phones and computers that can be customized by the purchaser? While the authorities believe Farook's Apple phone contains worthwhile data, the reality—from available reports in the media—seems that no one may really know. The authorities can find the phone numbers by use of metadata. The same metadata may also provide other intelligence. But what if Apple does comply and nothing is found? Who is going to pay for Apple's time and effort to hack its own technology whilst undermining its technological advantage and making a mockery of privacy? In the end there are probably more honest people who like their privacy than dishonest people who use privacy for personal gain.

5. Conclusion

This article examined some legal and technical issues pertaining to the right to privacy, with particular reference to the Microsoft and Apple cases. Recall that the impact of the judgements means all internet and cloud companies operating out of the U.S. may be required by the government to hand over content stored in other jurisdictions (nations) and firms may be compelled to decrypt devices. Of course this compulsion assumes decryption is possible and feasible, relative to the time value of the information sought. This poses a resultant risk to business viability as increased security will drive up client costs. Other businesses will go underground. There is the potential for increased cyber conflict as other nation-states copy the actions of U.S. security agencies.

The technical means of preserving privacy also proved to be potentially inadequate, depending on the trade-off between ease-of-use and security. Even if users preferred data security over ease-of-use, the legal issues raised above make any strong encryption a moot point if a user can be compelled to hand over the decryption key. Further, the effective mass-parallelization offered by quantum computing (once realized) would render such large-key encryption schemes almost instantly breakable (Rich & Gellman, 2014). Currently, quantum computer can only find the factors of small numbers, but it took less than 70 years for computing to shift tremendously in size (down) and power (up) from ENIAC to the mobile phone.

To sum up, corporations and individuals can protect their privacy by using encryption for the moment. Given that the purpose of encryption is to preserve privacy, how can compliance with any court order be measured in an effective way (i.e., how can a court determine that a corporation or individual has complied with an order?). Full compliance can't be measured without complete knowledge of the original information, prior to encryption. The Apple case is pertinent here as the FBI does have other avenues it can explore. A final thought: what if the phone in the Apple case contains nothing of relevance?

References

Australian Government Department of Defence. (2016). *2016 Defence white paper.* Available at http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf

Australian Law Reform Commission. (2014, June 30). *Serious invasions of privacy in the digital era.* Available at https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf

BBC. (2009, May 25). *Previous cases of missing data.* Retrieved from http://news.bbc.co.uk/2/hi/uk/7449927.stm

Bellovin, S. M., & Merritt, M. (1992). Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proceedings of the IEEE Symposium on Research in Security and Privacy* (pp. 72—78). Oakland, CA: IEEE.

Bergin, A. (2014, August 14). Terrorist risk means privacy must take back seat to security. *The Sydney Morning Herald.* Retrieved from http://www.smh.com.au/comment/terrorist-risk-means-privacy-must-take-back-seat-to-security-20140813-103kcu.html

Carroll, R. (2014, September 3). Judge may hold Microsoft in contempt after refusal to hand over foreign data. *The Guardian.* Retrieved from http://www.theguardian.com/technology/2014/sep/03/microsoft-contempty-court-judge-data-dispute

Cook, T. (2016, February 16). A message to our customers. *Apple Inc.* Available at http://www.apple.com/customer-letter

Davidson. (2009). *The law of electronic commerce.* Cambridge, UK: Cambridge University Press.

Doswell, R. (2015, July 29). Understanding ethical hacking in IT security. *ITPro Portal.* Retrieved from http://www.itproportal.com/2015/07/29/understanding-ethical-hacking-it-security/

Fakhoury, H. (2012, March 7). A tale of two encryption cases. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/deeplinks/2012/03/tale-two-encryption-cases

Fowler, A., & Cronau, P. (2013, May 29). Hacked! *Four Corners.* Retrieved from http://www.abc.net.au/4corners/stories/2013/05/27/3766576.htm

Gretch, D. (2015, June 19). Fast-growing cybersecurity program probes 'ethical hacking. *FIU News.* Retrieved from https://news.fiu.edu/2015/06/fast-growing-cybersecurity-program-probes-ethical-hacking/89551

Gribbin, J. (2013). *Computing with quantum cats: From colossus to qubits.* London: Random House.

Hern, A. (2014, March 21). Microsoft tightens privacy policy after admitting to reading journalist's emails. *The Guardian.*

Retrieved from http://www.theguardian.com/technology/2014/mar/21/microsoft-tightens-privacy-policy-journalists-emails

Hoffman, L. S. (1999). Removal jurisdiction and the all writs act. *University of Pennsylvania Law Review, 48*(2), 401—471.

Hollister, S., & Guglielmo, C. (2016, February 26). How an iPhone became the FBI's public enemy number one (FAQ). *CNET*. Retrieved from http://www.cnet.com/au/news/apple-versus-the-fbi-why-the-lowest-priced-iphone-has-the-us-in-a-tizzy-faq/

Johnstone, M. N. (2009). Security requirements engineering—the reluctant oxymoron. In *Proceedings of the 7th Australian Information Security Management Conference*. Perth, Western Australia: Edith Cowan University.

Kharpal, A. (2015, June 17). Ethical hacking: Are companies ready? *CNBC*. Retrieved from http://www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html

Kleinjung, T., Kazumaro, A., Jens, F., Arjen, L. K., Thomé, E., Bos, J. W., et al. (2010). Factorization of a 768-bit RSA modulus. In *Proceedings of Advances in Cryptology—CRYPTO 2010* (pp. 333—350). Berlin: Springer-Verlag.

Lum, M. (2004). *Offshore outsourcing and information confidentiality*. Bethesda, MD: SANS Institute.

Mansfield-Devine, S. (2013). Interview: Jon Callas, Silent Circle. *Network Security, 2013*(9), 17—20.

Mason, R. (2011, January 12). *Cloud storage cost comparisons: How the price of cloud storage compares to traditional storage*. Retrieved from http://www.nasuni.com/blog/39-cloud_storage_isnt_cheap_how_the_price_of_cloud

McCullagh, D. (2007, December 14). Judge: Man can't be forced to divulge encryption passphrase. *CNET*. Retrieved from http://www.cnet.com/news/judge-man-cant-be-forced-to-divulge-encryption-passphrase/

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *Special Publication 800-145 of the National Institute of Standards and Technology*. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft. (2016, January). *Privacy statement*. Available at https://privacy.microsoft.com/en-us/privacystatement

Pinsent Masons. (2007, October 2). *Law requiring disclosure of decryption keys in force*. Retrieved from http://www.out-law.com/page-8515

Rahman, R. (2012). Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. *Computer Law and Security Review, 28*(4), 403—415.

Reuters. (2016, February 18). *Apple rejects court order to help FBI unlock San Bernardino shooter's iPhone*. Retrieved from http://www.abc.net.au/news/2016-02-17/apple-ordered-to-aid-in-unlocking-california-shooters-phone/7177842

Rich, S., & Gellman, B. (2014, January 2). NSA seeks to build quantum computer that could crack most types of encryption. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html

Rushe, D. (2014, September 2). Apple blames 'very targeted attack' for hack of nude celebrity photos. *The Guardian*.. Retrieved from http://www.theguardian.com/technology/2014/sep/02/apple-denies-hacker-celebrities-naked-photos-icloud

Schneier, B. (1996). *Applied cryptography*. New York: Wiley.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York: Wiley.

Sifry, M. (2011). *WikiLeaks and the age of transparency*. New York: OR Books.

Shostack, A., & Stewart, A. (2008). *The new school of information security*. Upper Saddle River, NJ: Addison Wesley.

Steinman, J. (2000). The newest frontier of judicial activism: Removal under the All Writs Act. *Boston University Law Review, 80*(3), 773—883.

Stevens, T. (2009, February 25). *Debunking a myth: If you have nothing to hide, you have nothing to fear*. Retrieved from http://www.computerweekly.com/blogs/the-data-trust-blog/2009/02/debunking-a-myth-if-you-have-n.html

Stuart, K. (2014, September 3). How to protect your digital photos from hackers. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/sep/03/how-to-protect-your-digital-photos-from-hackers

United States v. New York Telephone Co., 434 U.S. 159 (1977). Available at https://supreme.justia.com/cases/federal/us/434/159/

Vatis, M., & Novack, J. A. (2014, June 10). *Memorandum of law in support of Verizon Communications Inc.'s motion to participate as amicus curiae and Microsoft Inc.'s motion to vacate search warrant*. Retrieved from http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Verizon%20Amicus%20Brief%20(Final).pdf

Zetter, K. (2013, March 15). Federal judge finds national security letters unconstitutional, bans them. *Wired*. Retrieved from http://www.wired.com/2013/03/nsl-found-unconstitutional/