2014

I remember Richelieu: Is anything secure anymore?

Michael G. Crowley
Edith Cowan University, m.crowley@ecu.edu.au

Michael N. Johnstone
Edith Cowan University, m.johnstone@ecu.edu.au

DOI: 10.4225/75/57a833d7c833e
Originally published in the Proceedings of the 7th Australian Security and Intelligence Conference, Edith Cowan University, Perth, Western Australia, 1-3 December, 2014

I REMEMBER RICHELIEU: IS ANYTHING SECURE ANYMORE?

Michael G. Crowley and Michael N. Johnstone
Edith Cowan University Security Research Institute, Perth, Australia
m.crowley@ecu.edu.au m.johnstone@ecu.edu.au

Abstract
Petraeus-gate, hacked nude celebrity photos in the cloud and the recent use of a search and seizure warrant in the United States of America to seek production of customer email contents on an extraterritorial server raises important issues for the supposably 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 paper explores the legal and technical issues raised by the these matters with emphasis on the courts 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 in it concludes with suggestions for 'safe' storage of data.

Keywords
Law, Privacy, Security, Encryption, Cloud Services

INTRODUCTION
To Cardinal Richelieu has been attributed the statement 'Give me six lines written by the hand of the most honest man, I will find something in them which will hang him'. Recent events suggest Internet users might sear those words into their subconscious as they enter cyberspace. Complacency in web-use exposes web users to additional risks in a highly security conscious environment. Recent examples include revelations that nude photos stored in the Cloud (Stuart, 2014) have been the subject of a successful targeted hack despite assumed secure storage (Rushe, 2014) while General Petraeus failed to hide his 'personal love affair' whilst using the web and lost his job. The Petraeus and nude photo matters highlight the current risks associated with Internet use. These are not isolated cases. The BBC (2009) reported on thirteen cases (between 2007-2009) of data loss of medical records, prisoner records and defence personnel records. Recent events such as the aforementioned, suggest that the problem still exists. The web is also an increasingly valuable source of information for security agencies driven by the realisation 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. 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 *Microsoft E-Mail Case*, highlight 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 America to produce information stored in Ireland. An appeal has confirmed this decision. This paper uses a case study, the *Microsoft E-Mail Case*, to examine legal and technical issues of privacy and security with respect to storage of information on the Internet. This paper explores this mélange of law, technology and security concluding with options for 'safe' storage of Internet data.

LEGAL ISSUES
The *Microsoft E-Mail Case* and subsequent appeals 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, while 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 jurisdiction limitations was a key issue in the *Microsoft E-Mail Case* decision other factors worth considering also arose especially as this was one of the few cases that made it into the public arena (see, for example, 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.

While Petraeus-gate raised no jurisdictional issues, the nude photo hack ignores jurisdictional limitations. But jurisdictional limitations usually apply to the execution of a search and seizure warrant and that is what makes the *Microsoft E-Mail Case* important. The hypothetical web-user always faced 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 their data may not be safe no matter where it is stored.

Jurisdiction is generally state-based so that a legal instrument issued in the United States of America (USA) is limited to the territory of the USA. Mutual Legal Assistance Treaties (MLAT) provide an agreed process for service and execution of warrants seeking information from outside a states jurisdiction. The decision in the *Microsoft E-Mail Case* stepped around these treaties because the warrant was served within the USA. The essence of the judgement is that Microsoft is to deliver email content held in one of its servers in Ireland to a New York Court because the warrant was served on Microsoft in the USA. 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 recognised that the impact of the judgement means all Internet and cloud companies operating out of America may be required by the US 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. The search warrant required Microsoft to hand the email content over to the American court or breach American law (see, for example, Carroll, 2014). In complying Microsoft may or may not breach Irish law, but would almost certainly breach European Union data transfer laws.

This warrant is also jointly covered by various America 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. The warrant shifted the onus on production to Microsoft. This is because the warrant is a combination of search warrant as usually used in criminal proceedings and a subpoena, a writ requiring persons or things to be delivered to the court. The warrant also has inbuilt secrecy provisions unlike traditional search warrants where the occupant is usually present at the search unlike a hypothetical web-user.

Any assumptions by web users that data were secure and private is meaningless. Stevens (2009) has blogged on the fallacy that if you have nothing to hide you have nothing to fear. This was demonstrated when General David Petraeus, former head of the Central Intelligence Agency was forced to resign after evidence of an extra-marital affair was revealed in emails. What made the Petraeus case significant is that Petraeus was very, very careful – he had something he wanted to hide and it was not criminal. It could be inferred he knew about Richelieu. The emails to his lover were never sent. They were filed in a drafts folder that the lover accessed and read. As such the contents of the emails were never transmitted so they would be out of reach of any electronic signals eavesdropping agency (Whittaker, 2012). What undid Petraeus was his lover warning off others via the Internet leading to one of the receiptants alerting the authorities. Examination of the lover's emails revealed traces that led to General Petraeus's door and he was, figuratively, hung.

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 USA. While Microsoft is generally recognised 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 paper Microsoft has office locations in some 211 countries. (http://www.microsoft.com/en-us/worldwide.aspx) Microsoft also has a privacy statement (http://www.microsoft.com/privacystatement/en-us/core/default.aspx)>) but this may be rendered useless by the *Microsoft E-Mail Case*.

It is Microsoft's activities in cyberspace that are at the centre of the *Microsoft E-Mail Case.* While cyberspace may be a construct in the ether it has terrestrial accouchements such as data storage, chat rooms, files and on-line 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.. In Verizon Communications Inc.'s Motion to Participate as *Amicus Curiae* in Microsoft's appeal against the decision in the *Microsoft E-Mail Case* Vatis and Novack cite *Morrison v National Australia Bank Ltd.,* 561 US 247, 248; "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". (http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/06/10/National-Security/Graphics/Verizon%20Amicus%20Brief%20(Final).pdf)

Judge Francis gave greater weight to the necessities of law enforcement over traditional concerns of jurisdiction and privacy. These concerns were covered in the recently published Australian Law Reform Commission report on *Serious Invasions of Privacy in the Digital Era*. This report observed that invasions of digital privacy occur with 'increasing ease and frequency (17) and 'personal information, once put online seems impossible to destroy or forget' (17). It went on to note that despite legal protections there are 'significant inconsistency in the law between jurisdictions' (26). The report recommended federal legislation to ensure consistency across Australia (278). Additionally the report recognised the potential impact of surveillance on important freedoms and liberties (277 per Professor Neil Richards) noting 'it can chill the exercise of our civil liberties' causing people to 'self adjust their behaviour even if they are not doing anything wrong' (277 per Associate Professor Moira Paterson).

TECHNICAL ISSUES

Cloud computing represents a natural evolution of information technology service provision, where 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 is perhaps a further stage of the outsourced information technology (IT) model of a decade ago. As with any new concept, there is often confusion as to what business value "the cloud" represents and therefore the quantifiable benefits that might accrue from the use of such technology are unclear. This section presents a definition of cloud computing, displays common cloud architecture and considers the impact of the need for security and privacy on cloud computing.

Cloud computing, at first glance, appears to be focused on large-scale storage of information, however, Mell and Grance (2011, p2) provide a succinct definition of cloud computing that encompasses more than storage, viz: "…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".

Vendors of cloud services assert that costs are lower than conventional models of IT provision, as low as 12 cents per Gb of storage per month, for example (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, cost is not, and should not, be the sole driver. Security of intellectual property and the need to keep valuable business data private are also key objectives for most firms, should they wish to keep their hard-won market share. The well-documented recent case of the MineLab metal detectors (Fowler, 2013) where the firm found their product had been copied and was being sold without their knowledge serves to highlight the seriousness of the problem.

The need for security and privacy is made more difficult as noted by Shostack and Stewart (2008), 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" (Shostack and Stewart, 2008, p89). This would likely be multiplied as the environment in which the software operates (e.g., cloud computing) becomes more complex. Put another way, 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 often is invisible). As software becomes ubiquitous, this reliance on software that may be insecure raises concerns in terms of business continuity.

Confidentiality is considered a core principle of information security. 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 façade as part of "software as a service". This describes the scenario where all of the cloud service layers function flawlessly to provide the expected (paid for) services. How would an attack on confidentiality affect the provision of cloud services? There may 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 disgruntled employees, lone hackers, activist groups, business competitors or nation-states. Much of the software required for these attacks is freely available. This suggests that businesses need the freedom to protect their information assets from others with appropriate security and privacy measures if they wish to have control over their intellectual property.

The metadata retention proposal by the Australian Government (Bergin, 2014), whilst viewed with dismay by telecommunications providers may not be completely anathema. Telstra, at least, did not see a problem with the proposal. 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 (on the 31st of July, 2014) 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 USA.

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 USA, the obvious option is a cryptographic method such that encrypting is easy but decrypting without the appropriate key is computationally infeasible. As mentioned previously, confidentiality is a core tenet of information security. The metadata retention proposal and the action by Microsoft present two different problems. The former, one of tracking where someone has been (potentially an attack on privacy), the latter an attack on confidentiality. Metadata retention is perhaps less of a problem for businesses as this may show what web site was visited by an employee, but not what s/he did whilst there. This leaves the latter, more serious problem, of assuring confidentiality.

A conventional approach to guaranteeing confidentiality involves encrypting the data at the source and decrypting it at the destination. This is commonly done with asymmetric encryption, where two keys are generated, a private key (held securely by the destination) and a public key (made available to anyone). If the keys are large enough, it can 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 a reasonable trade-off.

Are there any issues with this scheme? The keys must be related to large prime numbers. It takes time to find large (relatively) prime numbers. By large, we mean hundreds of decimal digits. It is obvious by inspection that 11 is a prime number as it has no factors other than 1 and itself. What about 524,287? How easy would it be to confirm 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. It also takes time to encrypt and decrypt messages. Ultimately, the users must decide the trade-off between time/security and convenience.

DISCUSSION

Davidson argues that the rules needed for cyberspace cannot be based upon the rule of law notwithstanding the parallels. (Davidson, 2009, 16) This is because the 'rule of cyberspace is the natural, emergent order arising from data chaos'. (Davidson, 18) Information in cyberspace has different values to different people with cyberspace providing freedom and order for users. (Davidson, 23) Davidson believes any attempt to control cyberspace will fail because of the special ability of cyberspace. (Davidson, 24)

Microsoft's failure to date in its challenge of the warrant pose serious risks to individual privacy and serious commercial risks for Microsoft. Whether or not Microsoft wins US security agencies have forced businesses to review security and privacy arrangements. Carroll (2014) has reported that the German government has 'told Microsoft it will shun data storage from US companies unless the ruling is overturned'. Foreign users and domestic Americans may well join the Germans and stop using American Internet services, a move that could impact adversely on 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 USA.

When you add the particular features of Petraeus-gate and the nude celebrity photo hack 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 maybe their email content stored outside of the USA can be easily accessed without their knowledge by American security agencies. Petraeus-gate tells us that these same agencies can with the tools available legally find you even if you want to stay private while the nude celebrity photo hack poses the question, how secure is secure?

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)? The unfortunate answer is "it depends". Before deciding 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 these data.

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, 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 confidentiality is maintained.

Ultimately, in the security chain, it is the human element that is the weakest link as demonstrated in Petraeus-gate. Wikileaks and the Snowden case (Sifry, 2011) also provide strong evidence towards this assertion. 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.

CONCLUSION

This paper examined some legal and technical issues pertaining to the right to privacy, with particular reference to the Microsoft case. Recall that the impact of the judgement means all Internet and cloud companies operating out of America may be required by the US government to hand over content stored in other jurisdictions (states). This poses a resultant risk to business viability as increased security will drive up client costs. Others businesses will go underground. Some business clients will want change so as not to be hung by Richelieu. There is the potential for increased cyber conflict as other nation states copy the actions of US 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 future realisation of quantum computing would render such large-key encryption schemes almost instantly breakable (Rich and Gellman, 2014).

Perhaps the final words belong to a cryptographer. They describe how technology was initially hailed as the saviour of privacy, but some critical self-reflection over time declares otherwise. "It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics" (Schneier, 1996). His view changed somewhat five years later. "It's just not true. Cryptography can't do any of that." (Schneier, 2000).

REFERENCES

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

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, Septermber 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

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

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

Johnstone, M.N. (2009). "Security Requirements Engineering-The Reluctant Oxymoron." *Proceedings of the 7th Australian Information Security Management Conference*, Edith Cowan University, Perth Western Australia, 1st-3rd December 2009.

Kleinjung Thorsten, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman Te Riele, Andrey Timofeev, and Paul Zimmermann (2010). Factorization of a 768-bit RSA modulus. CRYPTO'10 Proceedings of the 30th annual conference on Advances in cryptology. pp.333-350. Berlin: Springer-Verlag.

Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing. Special Publication 800-145. National Institute of Standards and Technology. Gaithersburg, MD: NIST.

Mason, R. (2007, January 12). Cloud Storage Isn't Cheap: How the Price of Cloud Storage Compares to Traditional Storage [Blog comment]. Retrieved from http://www.nasuni.com/blog/39-cloud_storage_isnt_cheap_how_the_price_of_cloud

Rich, S. and 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, Septermber 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. and Stewart, A. (2008). *The New School of Information Security*. Upper Saddle River, NJ: Addison Wesley.

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

Stuart, K. (2014, Septermber 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

Whittaker, Z. (2012, November 13). Yes, the FBI and CIA can read your email. Here's how. ZDNet. Retrieved from http://www.zdnet.com/yes-the-fbi-and-cia-can-read-your-email-heres-how-7000007319/

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/