The Complex Web: The Global Network, Snowden, Safe Harbours, Shields and the GDPR

Daniel Cater; BNSc (Dis), Juris Doctor (Hon), Phd student UNSW

INTRODUCTION

Data production is inherent in the internet. Myriad devices constantly produce huge volumes of data as part of everyday living in the information age and this data moves and is stored in servers and 'clouds' regardless of territorial borders. Logging onto a device and connecting to the internet produces data as both input and output, it can include everything from transaction and communication records to timestamps and location and it may be intentional or coincidental.[1] In the digital environment data moves rapidly and unpredictably, it can move in segments and be stored in multiple locales, it can be conglomerated with unrelated data, and data locality can be completely separate from involved parties.[2] Data often travels beyond either the control or knowledge of concerned parties, who have little or no influence over it, and it can be remotely accessed from sites hugely distant of its physical location.[3] The production of data has become an unavoidable aspect of integration into the modern world; this data is generated in massive volumes and can be moved, stored and accessed anywhere on the planet.

The production of data has become an unavoidable aspect of integration into the modern world; this data is generated in massive volumes and can be moved, stored and accessed anywhere on the planet

The rapid transfer and storage of data is essential to global communication and economies but it also presents threats to the security of that data as well as privacy; benefits and risks which increase as networking technology develops. Governments and international bodies have all recognised the critical role which rapid and efficient international data flow plays in economies, international development and global stability as well as the potential security and privacy threat it represents.[4] In Australia, Europe and across North America individuals, organisations and governments are all critical users of the global internet and must address its benefits and risks.

THE SNOWDEN EFFECT AND SCHREMS

In 2013 Edward Snowden, a US intelligence contractor, leaked documents revealing massive government surveillance programs with international reach; disclosures which caused worldwide anger and condemnation. The Snowden revelations related to widespread mass surveillance by the US and its allies, in particular its 'Five Eyes' treaty partners[5], provoked public debate and outraged privacy advocates.[6] Recent studies have indicated the Snowden leaks have reduced trust in data integrity and privacy online and resulted in reductions in both economic activity and internet free speech.[7] The Snowden leaks have thus become a watershed in changing social perception of government surveillance and formed a rallying point in demands for greater transparency and privacy protections online.[8] Individuals across the world now have height-

1 Schneier, Bruce, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company, 2015), p15-20.

2 Daskal, Jennifer, 'The Un-Territoriality of Data' (November 2015) 125(2) *The Yale Law Journal* 326, p366-78.

3 Ibid p333, 357, 369-74.

4 Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' UN Doc A/HRC/27/37 (30 June 2014); Organisation for Economic Co-operation and Development [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (11 July 2013) http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf; The Executive Office of the President 'Big Data: Seizing Opportunities, Preserving Values' (Review, The White House, May 2014); Department of Foreign Affairs and Trade, *FTA Chapter Summaries*, Trans-Pacific Partnership Chapter Summary: Electronic Commerce (12 November 2015) http://dfat.gov.au/trade/agreements/tpp/summaries/Documents/electronic-commerce.PDF

5 The Five Eyes group are the nations of Australia, Canada, New Zealand, the United Kingdom and the United States of America which have a series of bilateral intelligence and communication sharing agreements with their origin in the 1946 UKUSA Agreement; http://www.asd.gov.au/partners/allies.htm & https://www.nsa.gov/public_info/declass/ukusa.shtml.

6 Milanovic, Marko, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (Winter 2015) 56(1) *Harvard International Law Journal* 81, p81-2.

7 Goldberg, Rafi, 'Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities' (13 May 2016) *National Telecommunications & Information Administration Blog* https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities; Penney, Jonathon W., 'Chilling Effects: Online Surveillance and Wikipedia Use' (May 2016) *Social Science Research Network* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

8 Raab, Charles D., Richard Jones and Ivan Szekely, 'Surveillance and Resilience in Theory and Practice' (2015) 3(2) *Media and Communications* 21, p34-5.

ened awareness of the reach which bulk data surveillance operations have and are demanding action from the governments and corporations.

One major impact of this increased disquiet over transborder data surveillance and privacy protection has been in the *Schrems Case*[9] decision in 2015 which saw the European Court of Justice (**ECJ**) overturn the US/EU *Euro Safe Harbor*[10] provisions. Mr Schrems, an Austrian, challenged Facebook's European division arguing that data transferred to Facebook's main US servers did not receive the privacy protections required in the *European Human Rights Charter* (**ECHR**).[11] The ECJ decision centred on the *Euro Safe Harbor* ruling which determined the US met the threshold which allowed data transfers outside European borders to nations which adequately protected EU citizens' rights.[12] The ECJ acknowledged that privacy is not an absolute right and must give way to the proportional needs of national security and also stated that exponential technology growth has increased the vulnerability and concerns surrounding transborder data protection.[13] The ECJ then delivered a landmark ruling holding that, given the different protection afforded US and non-US residents, the US national security data surveillance policies were not proportionate to needs and failed to provide EU citizens with basic remedies and protections.[14] The ECJ decision highlights the critical, controversial and complicated nature of privacy rights, transborder data flow, surveillance powers and jurisdiction in the information age.

While the US has been forced to address its broad domestic surveillance powers many of the provisions related to collection of foreign data remain intact. Domestically the most notable reform was the curtailing of the controversial surveillance powers enshrined in the post 9/11 *USA Patriot Act*[15] with the passing of the *USA Freedom Act*[16] in 2015. Despite these reforms the *Patriot Act's* foreign surveillance reach remained largely intact.[17] Several other provisions permitting aggressive foreign data surveillance programs also remain in place, most notably *FISA* Section 702[18] and *EO12333*[19], both legislative tools which have been foundational in US extraterritorial bulk data collection operations.[20]

The international backlash demonstrated by the ECJ *Schrems Case* decision has begun to be felt in US policy with proposed laws to limit foreign surveillance, support transparency or provide redress options. One particular example, the recently passed *Judicial Redress Act*[21], provides non-US citizens with limited redress for privacy breaches in US law, an act which directly addresses one objection in the ECJ decision; that EU citizens do not have redress rights under US law.[22] Within the US administration other figures have recognised the international ramifications of the current US foreign data policies and have proposed fur-

9 *Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd* (C-362/14) [2015] Court of Justice of the European Union.

10 *European Parliament Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* [1995] *OJ L 281/31* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

11 O'Brien, Danny, 'No Safe Harbor: How NSA Spying Undermined U.S. Tech and Europeans' Privacy' (5 October 2015) *Electronic Frontier Foundation* https://www.eff.org/deeplinks/2015/10/europes-court-justice-nsa-surveilance and Fioretti, Julia, 'EU-U.S. data-sharing deal faces major challenge in EU court' (21 September 2015) *Reuters, Technology online* http://www.reuters.com/article/2015/09/21/us-ireland-eu-privacy-idUSKCN0RL15K201509211.

12 *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce* [2000] OJ L 215 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

13 *Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd* (C-362/14) [2015] Court of Justice of the European Union, para 10, 12-3.

14 Ibid para 22, 31, 90, 93, 95.

15 *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*.

16 *The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015*.

17 Froomkin, Dan, 'USA Freedom Act: Small Step for Post-Snowden Reform, Giant Leap for Congress' (3rd June 2015) *The Intercept_Unofficial_Sources* https://theintercept.com/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress/

18 *The Foreign Intelligence Surveillance Act of 1978* and *The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*.

19 *Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp, p. 200* http://www.archives.gov/federal-register/codification/executive-order/12333.html

20 Buchsbaum, Emma, 'Section 702:Programmatic Collection and the Wall Reprised' (26 April 2016) *Lawfare, Surveillance, Online* https://www.lawfareblog.com/section-702-programmatic-collection-and-wall-reprised and White, Nathan, 'We Need to Know More About When the FBI Can Access One of the NSA's Biggest Databases' (29 March 2016) *Just Security Online* https://www.justsecurity.org/30300/rules-fbi-access-12333/.

21 *The Judicial Redress Act of 2015*

22 Sensenbrenner, Rep Jim, 'The Judicial Redress Act is essential to U.S. law enforcement' (17 September 2015) *The Hill online* http://thehill.com/blogs/congress-blog/homeland-security/253874-the-judicial-redress-act-is-essential-to-us-law.

23 Trujillo, Mario, 'House members push bill limiting gov access to emails stored overseas' (27 February 2015) *The Hill online* http://thehill.com/policy/technology/234121-house-members-drop-bill-limiting-gov-access-to-overseas-email and Koh, Harold Hongju, 'Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights' (19 October 2010) United States Department of State Office of the Legal Advisor found at https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf, p55-6.

ther reforms.[23] Nevertheless while the US government has curtailed some of the laws permitting bulk data surveillance these reforms largely focus on the domestic provisions, with slower progress on reform of powers concerning foreign data surveillance.

Understanding the political and social consequences of the Snowden leaks and the subsequent US–EU legal arguments and legislative changes, such as the GDPR, is essential in this complex area

The importance of transnational data flows has been recognised by EU and US power brokers as critical and an EU/US compromise agreement, known as the *EU-US Privacy Shield* has been negotiated, but despite these efforts EU authorities remain sceptical. One influential EU privacy advocate stated that "No one wants data transfers to stop…" but that "…information on European citizens…" cannot "… be completely without protection when they [it] leave[s] Europe".[24] The current draft of the *EU-US Privacy Shield* has been reviewed by European privacy and legal experts and its status is uncertain with the nominated Article 29 review party highlighting important concerns.[25] These apprehensions have been mirrored by the European Data Protection Supervisor who stated that the *EU-US Privacy Shield* is not robust enough to endure the inevitable legal challenges, in particular given impending EU data protection reform.[26] It remains an open question whether and when any long-term agreement on data traffic between the EU and US will be found satisfactory but the newly finalised *European General Data Protection Regulation*[27] (*GDPR*) will certainly impact the process.

THE EUROPEAN GENERAL DATA PROTECTION REGULATION

The European Union has reviewed its regional data protection and privacy regulations and passed an updated regulation which will commence legal force in 2018. The *GDPR* has been passed and will enter into force across EU states from May 2018; it is envisaged to both increase EU citizen data protection and to encourage an integrated digital economy.[28] The *GDPR* includes provisions which shield EU citizens' data globally and assert responsibilities to companies beyond Europe's borders in the management and 3rd party sharing of EU data resources.[29] The nature of these rules and the size of the EU population and economy mean that any US based or other international company wanting to access the European market will have to comply with the rules dictated in the *GDPR*.[30] The nature of the global network structure which has been established between Australia, Europe, North America and many other world economies is such that the *GDPR* will need to be considered in legal and political policy in all these jurisdictions.

The structure of the *GDPR* explicitly allows for data transfer agreements within the protective framework of the *ECHR* and further it preserves those agreements in place prior to its entry into force. The *GDPR* includes provisions for establishing international cooperation and safeguards, it preserves such agreements which existed and complied with EU law prior to its passing and it provides for extensive review and oversight.[31] The Article 29 review committee into the *EU-US Privacy Shield* released a statement that the status of any revised agreement must be further reviewed in 2018 following the *GDPR* entry into full legal force.[32] It is clear that any EU-US data sharing agreement will be required to meet the standards of the *GDPR* as it enters into effect and it will also impact other nations' interactions with data policies.

24 Fioretti, Julia, 'Europe's top privacy watchdog calls on firms to curb U.S. data transfers' (23 October 2015) *Reuters, Technology online* http://www.reuters.com/article/2015/10/23/us-europe-dataprotection-idUSKCN0SH1ZT20151023.

25 Gibbs, Samuel and agencies, 'Data regulators reject the EU-US Privacy Shield safe harbor deal, (14 April 2016) *The Guardian Technology online* https://www.theguardian.com/technology/2016/apr/14/data-regulators-reject-eu-us-privacy-shield-safe-harbour-deal. Full text of the EU-US Privacy Shield provisions is available here European Commission unveils EU-U.S. Privacy Shield (29 February 2016) *European Commission, Justice, Newsroom, Data Protection, News* http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm. Full text on the opinion is here *Article 29 Data Protection Working Party, 'Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision'* [13 April 2016] 16/EN WP238 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

26 European Data Protection Supervisor, 'Privacy Shield: more robust and sustainable solution needed' (30 May 2016) *European Data Protection Supervisor, Press release,* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf

27 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

28 The European Commission, 'Protection of Personal Data', (10 May 2016) Media Release *European Commission, Justice, Data Protection* http://ec.europa.eu/justice/data-protection/

29 Above n27, Art 3, 4, 44, 45, 46.

30 Gibbs, Samuel, 'European parliament approves tougher data privacy rules' (14 April 2016) *The Guardian, Tech, online* https://www.theguardian.com/technology/2016/apr/14/european-parliament-approve-tougher-data-privacy-rules

31 Above n27, Art 46, 47, 48, 49, 50, 51, 52, 54, 96.

32 Statement of the Article 29 Working Party on the Opinion on the EU- US Privacy Shield (13 April 2016) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf

AUSTRALIA, EUROPE AND THE GDPR

Australia is an important member of the 'Five Eyes' intelligence sharing alliance and was thus involved in the surveillance operations that were exposed by Snowden. Further, involvement in the global digital economy is critical to Australian interests. Australia is the largest 'Five Eyes' member in the southern hemisphere, and has been identified in media reports concerning both data collection and sharing with partner states, in particular the United States.[33] The draft Trans-Pacific Partnership (**TPP**) trade agreement involves a dozen countries including Australia and the US and is under review following negotiations; the agreement includes extensive data sharing provisions.[34] In TPP negotiations, Australia additionally included a Memorandum of Understanding with the US that any law extending privacy protections to foreign and non-US residents in certain countries will also provide coverage to Australian citizens.[35] While the TPP itself, like the *EU-US Privacy Shield*, remains an agreement under review, its content, and that of supporting documents, is indicative of the importance and complexity of transborder data protection.

Geographic isolation and localised laws and rights protections are increasingly irrelevant in a world where communication, business, entertainment, crime and every other facet of day-to-day life can occur online as part of the global network. The understanding and control of how data moves across borders and its value and vulnerability as a resource in business, security and privacy spheres is critical to successfully navigating benefits and risks going forward. Understanding the political and social consequences of the Snowden leaks and the subsequent US-EU legal arguments and legislative changes, such as the GDPR, is essential in this complex area.

33 Tim Leslie and Mark Corcoran, 'Explained: Australia's involvement with the NSA, the US spy agency at the heart of the global scandal' (19 November 2013) *ABC News Australia online* http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786

34 Trans-Pacific Partnership Agreement, 'Outcomes: Trade in the digital age' *Australian Department of Foreign Affairs* http://dfat.gov.au/trade/agreements/tpp/outcomes-documents/Pages/outcomes-trade-in-the-digital-age.aspx

35 Robb, The Hon. Andrew AO MP and Ambassador Michael B. G. Froman, 'Letter outlining Memorandum of Understanding Extending US foreign national privacy protections to Australians with regards to TPP Agreement' http://dfat.gov.au/trade/agreements/tpp/official-documents/Documents/australia-united-states-privacy-protection.PDF