USMP UNIVERSIDAD DE SAN MARTIN DE PORRES | FACULTAD DE DERECHO

VOX JURIS

Portal de Portales latindex

THE CONCEPT OF DATA PRIVACY LAW AND ITS APPLICATION TO THE INTERNET

Dan Jerker B. Svantesson
Dan_Svantesson@bond.edu.au
Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

Received:18 de junio de 2014 Accepted: 28 de junio de 2014

SUMARIO

ABSTRACT

In a society where data is the lifeblood, data privacy will inevitably play a central role. In this article, I will examine in some detail the concept of data privacy law and how it applies to Internet conduct. This is a dauntingly large topic and as a consequence, the selection of issues discussed has had to be somewhat eclectic

RESUMEN

En una sociedad donde los datos son el alma, la privacidad de los datos inevitablemente desempeñará un papel central. En este artículo, se examinará en detalle el concepto de ley de privacidad de datos y cómo se aplica a la conducta de Internet. Este es un

tema grande con grandes desafíos y como consecuencia de ello, la selección de temas ha tenido que ser algo ecléctica.

KEY WORDS

Personal information - privacy - legality - Internet - globalization - interaction humanizes

PALABRAS CLAVES

Datos personales - privacidad - legalidad - internet - globalización - interacción humana

INTRODUCTION

It seems impossible these days to pick up any Internet-focused law journal without finding at least some articles dealing with some data privacy-related topic - data privacy is very much the flavour of the month. That this is so is not surprising. As noted by Rotenberg already in 1996: 'Privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century.'[1]

In a society where data is the lifeblood, data privacy will inevitably play a central role. In this article, I will examine in some detail the concept of data privacy law and how it applies to Internet conduct. This is a dauntingly large topic and as a consequence, the selection of issues discussed has had to be somewhat eclectic. For example, the majority of examples included in the discussion below are drawn from Europe, the US and Australia.

DATA PRIVACY LAW - WHAT'S THE BIG DEAL?

The concept of data privacy is elusive indeed and attempts at a clear definition generally seem to have failed. Thus, it is no surprise that the concept of data privacy law also is difficult to define with clarity, and delineate with precision. Adding further to the problem is the fact that many key concepts commonly included, expressly or implicitly, in attempts at defining data privacy law are themselves hard to pin down. For example, data privacy laws could be seen to essentially involve the protection of 'personal data' or 'personal information'. However, as has been illustrated e.g. by Burdon and Telford, the concept of personal data/information is, itself, lacking a clear definition.[2]

1 James Gleick, 'Big Brother Is Us', The New York Times, 29 September 1996 <http://www.nytimes.com/1996/09/29/magazine/ big-brother-is-us.html?pagewanted=all&src=pm>.

2 Mark Burdon and Paul Telford, The conceptual basis of personal information in Australian privacy law, eLaw Journal: Murdoch University Electronic Journal of Law (2010) 17(1).

A further cause of some confusion is the geographical differences in terminology. Addressing this issue, Bygrave notes that: "In Europe, such law [what I here refer to as data privacy law] tends to be described as 'data protection law'. In North America, Australia, and New Zealand, the preferred nomenclature tends to be 'privacy law'."[3] The full extent of the confusion this causes only becomes clear when we consider the fact that, Europeans give a specific meaning to 'privacy law', different to 'data protection law':

"In some respects, data privacy [or data protection] canvasses more than what are typically regarded as privacy concerns. The rules aimed at ensuring adequate data quality are an example in point. In other respects, data privacy encompasses less than privacy per se. The latter has spatial, bodily, and perhaps psychological dimensions that are usually not directly addressed by data privacy law.[4] (internal footnote omitted)"

At any rate, as long as we remain vigilant to their unavoidable deficiencies, several useful articulations of data privacy law are worth noting. Put very simply, privacy could be said to mean the "right to be let alone".[5] Another possible definition is that privacy is "[t]he interest of a person in sheltering his or her life from unwanted interference or public scrutiny."[6] An even more sophisticated definition would be to say that privacy relates to "[m]aterial that so closely pertains to a person to his[/her] innermost thoughts, actions and relationships that he[/she] may legitimately claim the prerogative of deciding whether, with whom and under what circumstances he[she] will share it."[7] Looked at in terms of functionality, the following definition is useful: "Data privacy law specifically regulates all or most stages in the processing of certain kinds of data. It accordingly addresses the ways in which data is gathered, registered, stored, exploited, and disseminated."[8]

Perhaps neither of these definition could be said to be more correct than the others, but taken together they provide a rather clear picture of what we mean when we talk about data privacy and data privacy law. While acknowledging the extensive literature[9] that exists on

3 Lee A. Bygrave, Data privacy law: An international perspective (Oxford, Oxford University Press, 2014), at xxv.

4 Lee A. Bygrave, Data privacy law: An international perspective (Oxford, Oxford University Press, 2014), at 3.

5 S. Warren and L. Brandeis, The Right to Privacy, 4 Harvard Law Review 193 (1890).

6 P. Nygh and P. Butt, Butterworths Concise Australian Legal Dictionary (2nd edn, Sydney, Butterworths, 1998)

7 Australian Law Reform Commission, Unfair Publication: Defamation and Privacy, Report No. 11 (1979), at 110.

8 Lee A. Bygrave, Data privacy law: An international perspective (Oxford, Oxford University Press, 2014), at 1.

9 Consider e.g. R C Post, Three concepts of privacy, 89(6) Georgetown Law Journal 2087 (2001).

Dan_Svantesson@bond.edu.au

this topic and the numerous variations of the definitions above it provides, I will not here delve deeper into the question of definition.

One important aspect to keep in mind, however, is that privacy is an internationally recognised fundamental human right.[10] Nevertheless, our personal information is increasingly treated, both by ourselves and by others, as a commercial commodity in our information society. In light of this, and bearing in mind the increase in the number of data privacy laws, it is more than likely that the area of data privacy law will continue to develop as one of the most significant and urgent Internet law questions over the coming years.

This development is caused by several factors such as:

a.- the globalisation of human interaction;
b.- the increasing commercial emphasis on data (companies such as Google and Facebook are built entirely on the data they hold); c.- the increasing governmental interest in data;
d.- the increase in voluntary data sharing such as people posting, or otherwise distributing, their personal information on social networking sites;
e.- the mentioned increasing 'commodification' of personal information (for example, many online services are provided for 'free' due to the data users provide - personal information is the currency used to pay for those services); and
f.- the increasing emphasis on privacy as a human right, protected under, for example, the ICCPR (Article 17) and its inevitable clash with partly competing human rights such as freedom of speech.

To this we may add the complications stemming from the fact that we have entered an era of so-called cloud computing[11] where the geographical location of data may not be clear, or as one commentator puts it "an era of cloud computing which disregards physical borders."[12] However, the impact of cloud computing should not be overstated. As noted by Kuan and Millard:

"While the popular view seems to be that in cloud computing data moves around the world continuously and almost randomly, so that it's not possible to know where a specific user's data are located at any one time [...], in practice this is often not so. In most cases,

10 See, eg, International Covenant on Civil and Political Rights, GA Res 2200A (XXI), 21 UN GAOR Supp No 16, UN Doc A/6316/1966, 999 UNTS 171 (entered into force 23 March 1976), art 17 ('ICCPR') and the Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), as amended by Protocols No 11 and No 14 (Rome, 4.XI.1950) ('ECHR').

11 For a discussion of privacy issues arising in the setting of cloud computing, see, eg, Dan Svantesson and Roger Clarke, 'Privacy and Consumer Risks in Cloud Computing' (July 2010) 26(4) Computer Law and Security Review 391-7.

12 Clare Sullivan, Protecting digital identity in the cloud: Regulating cross border data disclosure (2014) 30(2) Computer Law and Security Review 137-152, at 152.

data are usually copied or replicated to different data centres, for business continuity/backup purposes, rather than being 'moved' by being deleted from one data centre and re-created in another. Also, the primary copy of a set of related data [...] will often be stored in the same data centre. This will typically be the one geographically closest to the user in question, for latency reasons (speed of access and response for users), albeit perhaps data may be stored in fragments distributed amongst different storage hardware within that data centre. Often the provider will know where a user's data fragments (eg for a particular application) are stored, at the data centre if not equipment level. However, in most cases, whether for security or other reasons, providers do not disclose to users their data's location.[13]"

Furthermore, in seeking to predict the future relevance of data privacy law in the Internet context, it is interesting to contrast it to its arguably most closely related field of law, that is, defamation law. Internet defamation law has gained a considerable amount of attention. However, few online businesses publish content that is potentially defamatory, and few of us are defamed online to such a degree that we are seriously contemplating embarking on expensive cross-border defamation litigation. In contrast, most if not all Internet businesses deal with personal information in one way or another and thereby risk being exposed to the data privacy laws of the countries from which their customers come, and most Internet users' personal information is collected, used and disclosed in one form or another through their everyday Internet use. This adds further to my inclination to suspect that the area of data privacy law will maintain its centre stage position in the coming years.

Despite all this, one frequently sees suggestions that privacy is a thing of the past. For example, already in 1999, the Chairman and former CEO of Sun Microsystems Scott McNealy stated: 'You have zero privacy anyhow. Get over it.'[14] In a similar vein, former Google CEO Eric Schmidt stated: 'If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place';[15] and worse still, Facebook's Chief Executive Mark Zuckerberg has declared the age of privacy to be over.[16] Without making excuses for such statements, one must remember that they are made by people whose entire business depends on downplaying data privacy. In other words, their obvious motives should be

13 W Kuan Hon and Christopher Millard, 'Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4' (2012) 9:1(25) SCRIPT-ed 8 [Queen Mary School of Law Legal Studies Research Paper No. 85/2011] <http://dx.doi.org/10.2139/ssrn.1925066>.

14 John Schwartz, 'As Big PC Brother Watches, Users Encounter Frustration', New York Times, 5 September 2001, C6.

15 Ryan Tate, 'Google CEO: Secrets Are for Filthy People' (4 December 2009) Gawker <http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people>. For a strong rebuttal of such claims, see: Daniel J Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745.

Dan_Svantesson@bond.edu.au

enough for people to recognise the self-interested nature of these statements.

In contrast, it is difficult to find any mitigating circumstances for academics taking such a line. Yet, some academics, perhaps in a search for the type of attention that controversy commonly brings, have opted to attack privacy as a major problem for society: 'The right to privacy is the adult equivalent of Santa Claus and unicorns. No one has yet been able to identify where the right to privacy comes from and why we need it. In fact, the right to privacy is destructive of our wellbeing.'[17] Indeed, the same academic commentator has suggested: 'Rather than highlighting the need for more privacy, modern technology, in fact, underlines its irrelevance: people are more likely to invite attention, than seek anonymity.'[18]

This type of misrepresentations have been current for some time; and, notwithstanding that what they propose is contrary to the evidence of facts, they have been met with some credence, particularly amongst those with a political agenda hostile to privacy. In the end, however, such suggestions lack foundation and are easily refuted, both by reference to empirical evidence of how people actually feel about privacy and by reference to logical reasoning.

Statistical evidence produced by Eurobarometer in 2011 shows that a majority of Europeans are concerned about the recording of their behaviour via payment cards, mobile phones and mobile Internet and that 70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected.[19] Further, it is clear that people in general feel a loss of control over their privacy with just over a quarter of social network users and less than one in five online shoppers feeling in complete control[20]

This results in a low level of trust: 'Less than one-third trust phone companies, mobile phone companies and Internet service providers (32%); and just over one-fifth trust Internet companies such as search engines, social networking sites and e-mail services (22%).'[21] In fact, this distrust is so deeply rooted that 62% of the

16 Bruce Schneier, Google and Facebook's Privacy Illusion (4 June 2010) Forbes.com <http://www.forbes.com/2010/04/05/google-facebook-twitter-technology-security-10-privacy.html?boxes=Homepagechannels>.

17 Mirko Bagaric, 'Privacy Is the Last Thing We Need', The Age (online), (22 April 2007) <http://www.theage.com.au/news/ opinion/privacy-is-the-last-thing-we-need/2007/04/21/1176697146936.html>.

18 Mirko Bagaric, 'Rights Must Yield to Community Prosperity : The Fallacy That Is a Strong Right to Privacy' in Brett Mason and Daniel Wood (eds), Future Proofing Australia : The Right Answers for Our Future (Melbourne University Press, 2013) 65-80.

19 European Commission, Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> 1-3.

20 Ibid.

21 Ibid 2.

Dan_Svantesson@bond.edu.au

ISSN: 1812-6864

Europeans taking part in the survey give the minimum required information and 75% of them want to delete personal information on a website whenever they decide to do so.[22] Similar results can be found in studies carried out around the world and are not specific to Europe or even to western culture. For example, a Japanese study highlighted that about 70% of social networking users are worried about privacy protection on the Internet.[23]

Furthermore, contrary to popular belief, it is not conclusively established that 'young people' do not care about privacy.[24] First of all, the figures above include the views of young people. Second, on those occasions adults actually bother to enter into a dialogue with them rather than presuming to know what young people think, privacy concerns are often expressed by young people. For example, at the Nordic Youth Internet Governance Forum held in Stockholm in June 2012, privacy was highlighted as one of the key concerns by the group of young persons present.[25] Finally, while admittedly an unscientific method to prove the point, those who take the view that young people do not care about privacy should perhaps consider how willingly their teenage children would give them access to their e-mail accounts, Facebook account or indeed, old fashion diaries - if young people have no concerns about privacy, they would have no problem willingly handing over such information to their parents, but I suspect that such voluntary abandonment of privacy would be rare indeed.

Apart from statistical evidence, the erroneous arguments about the death, and indeed evils, of privacy such as those presented above may be refuted by the following. To say that we do not need a right of privacy because our modern information society does not cater for privacy is akin to saying that we do not need a right to water in a desert - the removal of a fundamental right is justified by reference to the environment being hostile to, or making difficult the exercise of, such a right. Such reasoning is clearly flawed and does not appear generally accepted in any context. Indeed, the opposite is true. For example, no reasonable person would suggest that we should not seek to protect animals facing extinction by reference to the fact that protecting such animals is made difficult by the circumstances under which those animals live.

22 Ibid 1-3.

23 Ministry of Internal Affairs and Communications (Japan), White Paper on Information and Communications in Japan 2010 <http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2010/2010-index.html>.

24 See, eg, Angelka Adrian, 'How Much Privacy Do Clouds Provide? An Australian Perspective' (2013) 29 Computer Law and Security Review 48, 56 stating, 'Younger generations have much less concern about online privacy than older generations.'

25 'The Nordic Youth IGF conference (NYIGF) was a pre conference to EuroDIG. Thirty youths in the age group of 14 - 17 years from Norway, Denmark, Iceland, Finland and Sweden formed the Nordic Youth Delegation. The NYIGF youth conference resulted in a number of recommendations regarding Internet governance': European Dialogue on Internet Governance Secretariat (EuroDIG), Messages from Stockholm (14-15 June 2012) <http://www.guarder.net/eurodig/2012/EuroDIG%20 2012_short_messages_to%20the%20IGF_final.pdf>.

Dan_Svantesson@bond.edu.au

In light of this, privacy - the 'ugly duckling' of the human rights - is more likely to continue to develop in importance than it is to become irrelevant, or indeed, to become destructive of our wellbeing.

Having established that data privacy is neither a dead issue, nor necessarily harmful to society per se, I hasten to add that I acknowledge the inherent competition between data privacy on the one hand and other societal values on the other hand. While obviously vulnerable to the criticism of oversimplification, assertions such as the following highlight important questions:

"At the heart of the issue is the question of tradeoffs: do we want more privacy in our data and, as a consequence, less efficiency and higher costs in the flow of data in commerce? Will we tolerate less security as a result of heightened restrictions on the access to our personal data that might be useful in combating crime or terrorism?[26]"

Reasonable people may disagree on how these questions ought to be answered. However, two observations may be made. First, the answer is not to be found in a complete abandonment of data privacy protection, and second, the exact correlation between the level of data privacy protection afforded in a particular society and the level of security risk that society experiences is a topic that must be approached with great care and without undue generalisations.

In the context of the public's attitude to data privacy law, it is interesting to look at that right from Olivecrona's perspective on rights.[27] Discussing the meaning, or lack thereof, of the terms "rights" and "duties", Olivecrona observed that:

> "The sentence that A is the owner of this piece of land functions as a permissive sign for himself with regard to this piece of land; at the same time it acts as a prohibitive sign for everybody else. The sentence is a green light for the owner, a red light for the others.[28]"

Applying this to privacy, the sad truth seems to be that one person's right of privacy far too seldom result in a red light for others. Indeed, as many people seem to struggle with what entitlements come with a right to privacy, the light that should have been green, may more

26 Edward C Harris, 'Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers' (2006-2007) 22 American University International Law Review 746, 746.

27 This discussion draws upon: Dan Svantesson, Fundamental policy considerations for the regulation of Internet cross-border privacy issues, Policy & Internet Vol. 3(3) 2011, Article 7 (2011).

28 Karl Olivecrona, Legal Language and Reality, in Essays in Jurisprudence in Honor of Roscoe Pound. Ed. R. A. Newman, 151-91. Indianapolis, IN: Bobbs-Merrill. 1962, at 183.

often be amber, signalling the risks associated with an unchartered territory. Further, it seems that a large section of the public simply ignores the light altogether in their use of Facebook and other social media. Put in other, perhaps clearer, words, people in general either have a too vague idea of what entitlements stem from their right of privacy, or fail to appreciate the importance of privacy. At the same time, businesses and others, in whom we entrust our most personal information, do not feel significantly restrained in how they use and abuse our privacy. Taken together, this combination results in an inadequate privacy protection, and if we return to Olivecrona's terminology, it could be said that we need clearer green lights and clearer red lights.

Conceded that all this is correct, we must move on to ask how we can achieve a clearer understanding and stronger respect for the right of privacy. Olivercrona's writings can aid us also in this regard. In discussing "performative utterances" such as promises made in a contractual situation, he notes that:

> "Their consequences are of a double nature. First, they have immediate, psychological effects. The promisor feels himself bound; the promise feels entitled to expect the promisor to act accordingly; contrary behavior is apt to provoke hostile reactions. Secondly, the acts correspond to certain requirements in the law; they are relevant in one way or another for actions by the state organs. Since the state organs regularly apply the rules, the promisor is likely to be exoposed to a sanction if he breaks his promise; his awareness of this fortifies the immediate psychological effect of the promise on him.[29]"

Olivecrona also notes that: "The green and red lights do not express any notions. They are signs which have a social function because these two observations, the effect a right has is consequently based on the immediate psychological reaction it causes and the extent to which the law enforces, and is seen to enforce, the right. The solution would then seem to lie in changing the psychological reaction to privacy rights, and applying law more effectively and visibly. Unfortunately, that is not always the case.[31]

---

29 Karl Olivecrona, Legal Language and Reality, in Essays in Jurisprudence in

Honor of Roscoe Pound. Ed. R. A. Newman, 151-91. Indianapolis, IN: Bobbs-Merrill. 1962, at 180.

30 Karl Olivecrona, Legal Language and Reality, in Essays in Jurisprudence in

Honor of Roscoe Pound. Ed. R. A. Newman, 151-91. Indianapolis, IN: Bobbs-Merrill. 1962, at 183.

31 For an interesting discussion of the importance of proper reporting, see: Greenleaf, GW., 2002, 'Reporting Privacy Complaints Pt 1: a proposal for systematic reporting of complaints in Asia-Pacific jurisdictions', in Privacy Law and Policy Reporter, vol 9(3), pp. 41 - 48; Greenleaf, GW., 2002, 'Reporting Privacy Complaints Pt 2: complaint reporting practices of Asia-Pacific Privacy Commissioners', in Privacy Law and Policy Reporter, vol 9(4), pp. 74 - 79; and Greenleaf, GW., 2002, 'Reporting Privacy Complaints Pt 3: complaint reporting practices of Canadian Privacy Commissioners', in Privacy Law and Policy Reporter, vol 9(6), pp. 111 - 115.

Dan_Svantesson@bond.edu.au

WHAT DATA PRIVACY LAW AIMS TO ACHIEVE

In his comprehensive study of data privacy law, Bygrave provides us with several important tools to better understand the core aims and functions of data privacy law. Here I will focus on the 'central rules of data privacy law' that his extensive international research has identified:

> The central rules of data privacy law embody a set of largely procedural principles. The core of these principles may be summed up as follows:
>
> a.- personal data should be collected by fair and lawful means (principle of fair and lawful processing);
> b.- the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is gathered and further processed (principle of minimality);
> c.- personal data should be collected for specified, legitimate purposes, and not used in ways that are incompatible with those purposes (principle of purpose limitation);
> d.- personal data should be relevant, accurate, and complete in relation to the purpose for which it is processed (principle of data quality);
> e.- personal data should be protected against unauthorized attempts to disclose, delete, change, or exploit it (principle of data security); [and]
> f.- processing of personal data should be transparent to, and capable of being influenced by, the data subject (principle of data subject influence).
>
> These are not the only principles found in data privacy law but they are central to it.[32] (internal footnote omitted)

In my view, if we allow ourselves to assume that the core principles do indeed carry out the aims of data privacy law, they give a clearer idea of what this area of law aims to achieve than does broad-brushed formal policy statements about the aim of this area of law, such as that found in Article 1 of Convention 108[33] outlining its principal object "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')."[34]

32 Lee A. Bygrave, Data privacy law: An international perspective (Oxford, Oxford University Press, 2014), at 1-2.

33 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No 108 (adopted on 28 January 1981).

34 Lee A. Bygrave, Data privacy law: An international perspective (Oxford, Oxford University Press, 2014), at 119.

GEOGRAPHICAL DIFFERENCES IN ATTITUDES TO DATA PRIVACY LAW

Discussions of differences in attitude towards privacy typically focus on the transatlantic chasm between Europe on the one hand, and the US on the other hand. That discussion is of particular importance as it is often seen to represent the two alternatives between which the rest of the world needs to choose. Thus, I will here make a few observations about the transatlantic differences.

However, first it is interesting to reflect on the available regulatory models in the data privacy arena. Moshell has identified four 'basic models for regulation of data protection'. They are:

a.- The comprehensive model - 'The comprehensive model allows for general laws governing collection, use, and distribution of information in a system in which an oversight body monitors both the private and public sectors to ensure compliance. [...] One variation of the comprehensive model is the co-regulatory model, in which industry takes an active role in both developing and enforcing rules for the protection of data privacy.'[35]

b.- The sectoral model - 'The sectoral model involves no general laws; rather it only targets those specific industries shown to be a threat to data privacy.'[36]

c.- The self-regulation model - 'Companies and industry bodies establish governance through codes and self-policing in the self-regulatory model.'[37]

d.- The privacy technologies model - 'Not so much a model of governance as a tool increasingly used by governments, privacy technologies enable individual users to take a hand in the accumulation and distribution of their own personal data. Encryption, anonymous remailers, proxy servers, and digital cash are examples of advances that would enable a proficient Internet user to protect his or her own data privacy.'[38]

As acknowledged by Moshell, none of these models are mutually exclusive 'as their complimentary or contradictory nature is dependant upon their application'.[39]

As to the transatlantic divide in attitudes towards data privacy, it has been noted that: 'A face-off between EU and U.S. data-protection positions [...] present an interesting scenario in which

35 Ryan Moshell, '...And Then There Was One: The Outlook for a Self-Regulatory United States amidst a Global Trend toward Comprehensive Data Protection' (2004-2005) 37 Texas Tech Law Review 357, 366.

36 Ibid 367.

37 Ibid.

38 Ibid (footnote omitted).

39 Ibid 366.

Dan_Svantesson@bond.edu.au

the world's largest consumer market and the world's largest economy, respectively, occupy extreme opposite ends of the dataprotection spectrum'.[40]

However, in the context of a trans-Atlantic comparison, it is interesting to start a bit further back in history, and it is important to bear in mind the role played by American scholars writing in the very earliest days of privacy. Already in 1890, Warren and Brandeis' crucially important article 'The right to privacy' introduced a call for a privacy right in light of the technological development at the time:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'[41]

The enormous influence this article has had is unquestionable. In fact, in surveying the most-cited law review articles of all time, Shapiro and Pearse found that Warren and Brandeis' mentioned article ranked second.[42]

At least two conclusions should be drawn from this. First, privacy is neither a European invention, nor is it an exclusively European concern. Second, technological developments have been a driving force for the push for privacy since the very conception of the idea of a privacy right.

Turning to privacy in the US today, several commentators are critical. For example, Moshell concludes:

> Taken as a whole, the U.S. system of self-regulation of data protection has proved to be fundamentally flawed. Without legislation that provides a solid support structure for what little government data-protection authority exists, the United States suffers from a general lack of enforcement that stems from industry disregard for voluntary data-protection concepts. Not only does this deficiency handicap the United States' effort to uphold what many consider

40 Ibid 359.

41 Louis Brandeis and Samuel Warren, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 195 (footnotes omitted).

42 Fred R Shapiro and Michelle Pearse, 'The Most-Cited Law Review Articles of All Time' (2011-2012) 110 Michigan Law Review 1483, 1489.

> to be a fundamental right, but because of the economic consequences, it also conceivably risks the United States' supremacy in a globalized economy.[43]

Greenleaf's assessment is that:

> The USA is best seen as a country with a unique, largely isolated, and sometimes inconsistent approach to data privacy, with some key standards weaker than is common in the rest of the world (particularly limits on collection, secondary use, disclosure, and data exports [ie the heartlands of European data privacy law]). But it also often provides international innovation in relation to some principles (eg data breach disclosure, and other aspects of security) and in the deterrent effect of draconian examples of enforcement, particularly by the FTC.[44]

In short, as noted by Cate: 'The protection for information privacy in the U.S. is far removed from that provided by the EU's data protection directive.'[45]

In 1970, Hesse - a federal state of Germany - passed the world's first data privacy Act. This was followed by the first such law on a national level being introduced in Sweden in 1973.[46] The European preoccupation with the right of data privacy, or data protection, stems at least in part from the horrendous experiences in Europe during the Second World War during which records of personal data were used for the purpose of identifying Jewish individuals.[47]

However, there is certainly also a commercial side to data privacy, and the European attitude to data privacy may be seen as an attempt to create a competitive advantage in an increasingly cutthroat world economy. As expressed by the Vice-President of the European Commission Viviane Reding: 'The new rules also give EU companies an advantage in global competition. [...] Trust in a coherent EU regulatory regime

---

43 Ryan Moshell, '...And Then There Was One: The Outlook for a Self-Regulatory United States amidst a Global Trend toward Comprehensive Data Protection' (2004-2005) 37 Texas Tech Law Review 357, 384 (footnotes omitted).

44 Graham Greenleaf, 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108' (2012) 2(2) International Data Privacy Law 68, 72. See also Graham Greenleaf and Nigel Waters, 'Obama's Privacy Framework: An Offer to Be Left on the Table?' (2012) 119 Privacy Laws and Business International Report 6-9.

45 Fred H Cate, 'The European Data Protection Directive and European-US Trade' (1998) 7 Currents: International Trade Law Journal 61, 73. While now slightly dated, this article provides an interesting comparison between US and EU data privacy law. See also, eg: Steven R Salbu, 'The European Union Data Privacy Directive and International Relations' (2002) 35 Vanderbilt Journal of Transnational Law 655. Directive 95/46/EC of the European Parliament and of the Council 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.

46 Datalag (Sweden) 1973:289.

47 Data Protection Commissioner, Section 1: What is Privacy? (14 November 2007) <http://www.dataprotection.ie/documents/ teens/cspe%20resource%20booklet/Section_2_-_Privacy_as_a_Human_Right.pdf>.

Dan_Svantesson@bond.edu.au

will be a key asset for service providers and an incentive for investors looking for optimal conditions when locating services.'[48]

While frequently emulated, the European approach to data privacy has also been subject to extensive criticism. For example, one commentator concludes that the EU approach places too much emphasis on privacy and thus has failed to strike an appropriate balance between privacy and the competing interests including the interests of free data flows and of security.[49] Further, the same author has argued that ECJ cases have shown that 'the rights extended to E.U. citizens by the [Data Protection] Directive fail to recognize the practical realities of how data is used in global commerce'.[50]

Discussing the Directive, Kuner notes that:

> The lack of widespread and consistent enforcement of data protection violations has a negative affect on the willingness of data controllers to comply with European data protection rules. [...] In the globalized economy, all factors affecting cost (including legal compliance burdens) tend to be subject to a risk management exercise, with compliance being more likely when the risks and costs of non-compliance are higher than those of compliance. Thus, in many cases data controllers may regard data protection rules as a kind of bureaucratic nuisance rather than as 'law' in the same category as tax and other laws, mainly because of the relative lack of enforcement and the relative mildness of the possible penalties.[51]

Importantly, he has also pointed out that:

> "Data protection law is a European success story that was ahead of its time and has since spread around the world. But the EU Data Protection Directive was enacted just before the Internet revolution and the globalization of data processing got underway, and thus requires rethinking and adjustment to retain its internal cohesion, and thus its effectiveness, for authorities, data controllers, and individuals alike.[52]"

48 Viviane Reding, 'The European Data Protection Framework for the Twenty-First Century' (2012) 2(3) International Data Privacy Law 119, 129. Importantly, Reding's assertion as to the competitive advantages to be gained from a well-structured data privacy framework has also been recognised by industry. See, eg: Peter Cullen and Jean Gonié, '1995 - 2012: from a Directive to a Regulation, the Microsoft Perspective' (2012) 2(3) International Data Privacy Law 117, 117.

49 Edward C Harris, 'Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers' (2006-2007) 22 American University International Law Review 746.

50 Ibid 798.

51 Christopher, The 'Internal Morality' of European Data Protection Law (November 24, 2008). Available at SSRN: http://ssrn. com/abstract=1443797 or http://dx.doi.org/10.2139/ssrn.1443797, at 9.

52 Christopher, The 'Internal Morality' of European Data Protection Law (November 24, 2008). Available at SSRN: http://ssrn. com/abstract=1443797 or http://dx.doi.org/10.2139/ssrn.1443797, at 19.

It will be interesting to see the extent to which the ongoing reform to the EU data protection framework will be better placed to deal with modern communications technologies.

In any case, the European attachment to data privacy is perhaps best illustrated by reference to the fact that 'the EU Charter on Human Rights adopted in 2000 by the Treaty of Nice has distinguished the Data Protection from the Privacy Right in order to consecrate the right of each EU citizen to have all his or her personal data protected[.]'[53]

More precisely, Article 8 of the Charter of Fundamental Rights of the European Union[54] addresses the protection of personal data and reads as follows:

a.- Everyone has the right to the protection of personal data concerning him or her.
b.- Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
c.- Compliance with these rules shall be subject to control by an independent authority.

This is complimented by the, in a sense more typical, Article 7 addressing the right of respect for private and family life: 'Everyone has the right to respect for his or her private and family life, home and communications.'

Background facts such as what has been presented above must be borne in mind when one approaches the modern treatment of data privacy. At the same time, it is encouraging to see what may be viewed as indications of a forthcoming convergence and harmonisation between the rather distinct approaches taken by the EU and the US.[55]

THE UNIQUE ON LINE ENVIRONMENT

The fact that the widespread uptake of information and communication technologies (ICT) has revolutionised the handling of personal information is beyond intelligent dispute. Indeed, countless journal articles and conference papers commence by pointing to this fact.

53 Yves Poullet, 'Transborder Data Flows and Extraterritoriality: The European Position' (2007) 2(3) Journal of International Commercial Law and Technology 141, 143 (footnote omitted).

54 (2000/C 364/01). The Charter only came into force 1 December 2009.

55 See further: Christopher Kuner et al, 'Moving Forward Together' (2012) 2(3) International Data Privacy Law 81.

Dan_Svantesson@bond.edu.au

Yet, there is currently a paucity of in-depth analysis of exactly how ICT has impacted upon the handling of personal information. A related and perhaps even more fundamental question, deserving of further attention, is the matter of what it is that makes the online environment different for the purpose of the handling of personal information. This part is devoted to that very question.

I have identified seven particularly important characteristics of ICT that individually, and in conjunction, cause significant changes to the handling of personal information. They are discussed in some detail below and include:

a.- Large data collections;
b.- Interconnectivity between networks;
c.- The border-disregarding nature;
d.- The ease of data distribution;
e.- The difficulty of data deletion;
f.- The ease of data searches; and
g.- The security difficulties.

I obviously acknowledge the subjectivity of this exercise and the impossibility of identifying and classifying all such characteristics. I have selected those characteristics I feel are of the greatest importance. Others may have opted to emphasise other characteristics. However, I think it is unlikely that anyone would disagree that the characteristics I have identified are of importance.

Large data collections

ICT makes possible the collection, storage, use and distribution of data on a previously unimaginable scale. And with increasing storage and processing power in ever smaller devices, combined with increased connection speeds, it can be anticipated that data collection, storage, use and distribution will only continue to increase.

Lately, 'Big data' has become a term of art referring to 'novel ways in which organizations, including government and businesses, combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both hidden information and surprising correlations'.[56]

Just how large quantities of data we are dealing with is clear from the below:

> "The Economist reports in its 2012 Outlook that the quantity of global digital data expanded from 130 exabytes in 2005 to 1,227 in 2010, and is predicted to rise to 7,910 exabytes in 2015.

56 Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 (2) International Data Privacy Law 74, 74.

> ['Welcome to the yotta world', The Outlook for 2012, Economist, Dec. 2011; http://www.economist.com/node/2 1537922.]
>
> An exabyte is a quintillion bytes. If you find that hard to visualize, consider this: someone has calculated that if you loaded an exabyte of data on to DVDs in slimline jewel cases, and then loaded them into Boeing 747 aircraft, it would take 13,513 planes to transport one exabyte of data. Using DVDs to move the data collected globally in 2010 would require a fleet of more than 16 million jumbo jets.[57]"

Where large quantities of data are being stored, such collections may, depending on the type of data, become 'honey pots' targeted by parties wanting to gain access to the data in question. Typical examples of honey pots include databases that include credit card information, user details, passwords etc. In other words, size is a problem in itself when it comes to data management, and perhaps it could be said that the larger the data collection the more attractive it is to third parties and, therefore, the more at risk it is.

Interconnectivity between networks

One of the greatest characteristics of the Internet is its ability to connect people. This comes naturally as the Internet is a 'network of networks' - a vast number of smaller networks connected together to make a very large network. It is, for example, due to the fact that Bond University's network is connected to the rest of the Internet that one can access the Bond University library catalogue from eg London, Las Vegas or Lima.

From a data protection perspective, this interconnectivity is clearly associated with risks. This is so not least due to the fact that typically as soon as a network is connected to the Internet, it can be accessed remotely and thereby it becomes vulnerable to access by parties that should not get access to the network.

The border-disregarding nature

The Internet was not designed with geopolitical borders in mind. At the same time, geography is by no means unimportant in the online context. In fact, geographical considerations are often as prevalent online as they are offline.

In light of this, it is unsurprising that Internet technology has developed so as to make possible the identification of the geographical location of Internet users ('geo-identification') through the use of so-called 'geo-location technologies'.

57 Christopher Kuner et al, 'Editorial: The Challenge of "Big Data" for Data Protection' (2012) 2 (2) International Data Privacy Law 47-49.

Dan_Svantesson@bond.edu.au

The existence of such technologies fundamentally challenges some key conceptions of the Internet and Internet regulation. In fact, geolocation technologies may play a central role in future schemes for dealing with cross-border Internet issues.

The ease of data distribution

It has been said that in the mid-1980s, Stewart Brand made the interesting observation that 'information wants to be free'.[58] While this statement may be associated with a degree of controversy, the ease with which information can be distributed is undeniable.

This ease of distribution significantly impacts data privacy; after all, data privacy is, in a sense, about restricting or controlling the movement of data.

The difficulty of data deletion

In 2007, Google launched its Google Street View ('Street View') system. Street View allows users to view panoramic images on a street level. The images for Street View were collected by driving cars equipped with a set of cameras along public roads taking photos that could be assembled to a seamless view of the streets.

As could be expected, images of people doing all sorts of things people do on public streets were captured. One particularly unfortunate image showed a woman stepping in or out of a car with the result that a substantial part of her bottom being visible in the image. When this was discovered, the image was removed by Google. However, prior to being deleted, the image had been copied and can be found online to this day.

While perhaps a rather mundane occurrence, this series of events shows us something important - once content is placed online, it may be difficult, or indeed impossible, to get it removed. This is of course closely related to the characteristic ease with which data is distributed discussed above, but it is also a characteristic that is deserving of attention in its own right.

For the woman in question to ensure that the image is removed permanently and completely from the Internet, she would need to identify all sources from which the image in question can be accessed. She would then need to contact all those sources and get their agreement to have the image removed. This is complicated by the omnipresent nature of the Internet which means that the sources may be geographically spread. It is also complicated by the fact that

58 Information Wants to Be Free (7 May 2013) Wikipedia <http://en.wikipedia.org/wiki/Information_wants_to_be_free>.

Internet content such as web pages and the images they hold are frequently backed up ('cached') eg by search engines.

In conclusion, there can be no doubt that the difficulty of deleting data significantly impacts data privacy.

The ease of data searches

Unstructured data is largely inaccessible data until it is searchable. The Internet is made up of both structured and unstructured data in a sense. However, as a whole the Internet is best viewed as being unstructured.

The widespread availability of relatively accurate search engines means that the unstructured data that makes up the Internet becomes accessible in a manner it would otherwise not be. And with this accessibility comes increased data protection risks.

The important role played by search engines came under the proverbial microscope in a recent decision by the Court of Justice of the European Union (CJEU).[59] The decision is highly relevant and worth considering in some detail.[60]

When Spanish citizen Mr Mario Costeja González, via a Google search, found links to two, for him unflattering, pages of the Spanish newspaper La Vanguardia from 1998, he requested that the newspaper remove the personal information about him contained in the relevant pages. He also requested that Google Spain and Google Inc remove or conceal the personal data relating to him so that the data no longer appeared in the search results and in the links to La Vanguardia.

The matter ended up before the Spanish data protection authority Agencia Española de Protección de Datos (AEPD). The AEPD rejected the complaint against La Vanguardia. At the same time, it upheld the complaint against Google.

Google brought the matter before the Spanish National High Court (Audiencia Nacional), and that court referred the matter to the CJEU.

As could be expected, the CJEU's decision is legally technical and many of the legal questions dealt with are specific to the

59 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Case C-131/12)

60 This part draws upon: Dan Svantesson, Google court ruling creates a more forgetful internet, The Conversation (14 May 2014) (https://theconversation.com/google-court-ruling-creates-a-more-forgetful-internet-26696).

Dan_Svantesson@bond.edu.au

European Union. However, the consequences of the decision are global. For example, the Court discussed in detail whether the functions carried out by Google Search amounted to data "processing", and whether Google was a data "controller" under the relevant EU law.

The Court answering both these questions in the affirmative meant that Google was responsible for its search results completely independently of the possible liabilities of the publishers, such as the newspaper in this case.

This means that even if certain content, such as the newspaper reporting relating to Mr Mario Costeja González, can lawfully be uploaded to the Internet, it may be unlawful for Google to list such content in its search results.

For the EU, there are practical advantages in such an approach. It means that, by controlling the search engines, it can affect at least the likelihood of personal information being found online even where the information is provided by a party located outside the EU:

"Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.[61]"

Perhaps the most serious aspect of the judgment relate to the so-called "right to be forgotten". The Court concluded that, where search results appear to be inadequate, irrelevant or no longer relevant, or excessive, the information and links concerned in the list of results must be erased. This applies even where the information is true and published lawfully by third parties. In other words, the Court places on Google the burden of deciding whether search results have become outdated.

The practical difficulties with this are obvious. First of all, there is the risk of search engines erring on the side of caution and removing any content complained of. After all, the risks of not removing the content may easily outweigh any perceived advantage of keeping the content accessible. Second, content may be seen to be outdated and irrelevant on one date only to become highly relevant again at a later date.

61 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Case C-131/12).

For example, information about a person's conduct may be seen to be outdated one day but become relevant again at a later date if that conduct is repeated. In other words, the relevance of information is not static - it is constantly changing and is always dependent on context.

In any case, the Court's conclusion on the right to be forgotten will no doubt reverberate across the world. Indeed, it forces the creation of a more forgetful internet.

From a privacy perspective this must be seen as a victory. But at the same time, privacy interests must always be balanced against competing interest such as freedom of information. The Court acknowledged this and stated that, while the right to be forgotten ordinarily trumps competing interests such as the economic interest of the search engine operator and the interest of the general public in finding information upon a search relating to the data subject's name: "That would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question."[62]

The question is of course how this assessment will work in practice.

The security difficulties

Time and time again we see evidence of the difficulty, some say impossibility, of keeping data secure. There have been several spectacular ICT security failures in just the recent years. For example, in 2011 SONY revealed that the personal information of approximately 75 million Play Station Network users had been compromised as a result of an illegal intrusion on its system. The aftermath of this intrusion is still on-going at the time of writing, with SONY dropping its appeal against a £250,000 fine issued by the UK Information Commissioner's Office as late as 13 July 2013.[63]

There is, unfortunately, a wealth of other examples of hacking incidences with major impact, and the only thing that is certain is that there is no end to such incidents in sight.

In 2014, the Australian Defence Signal Directorate brought attention to the following four trends that in combination will enhance the incentives for, and capability to conduct, malicious activity in cyberspace:

62 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Case C-131/12), at para 84.

63 Mike Suszek, Sony Drops Appeal for ICO-Issued 2011 Data Loss Fine (13 July 2013) Joystick <http://www.joystiq. com/2013/07/13/sony-drops-appeal-for-ico-issued-2011-data-loss-fine/>.

Dan_Svantesson@bond.edu.au

> Motivation is increasing. Australia's increasing reliance on the Internet is leading to more high-value information being stored and communicated on Australian government and commercial networks. This is boosting the incentive to undertake cyber crime or exploitation for direct monetary profit or indirect economic and political advantage.
>
> Capability is easier to acquire. Acquiring a cyber capability is becoming easier with increasingly sophisticated tools, information, and guidance readily available online.
>
> New technologies will generate new vulnerabilities. The proliferation of new technologies will increase the number of potential vulnerabilities. Of note, the growth in cloud computing and expanding use of mobile computing devices, such as smartphones, laptops and tablet computers, will generate more platforms—with distinct software, settings and applications—and more users to exploit.
>
> The spectrum of malicious actors is expanding. The ease of acquiring a cyber capability coupled with the potential high gains—whether financial, economic, diplomatic or political—is enticing more actors into malicious cyber activity.[64]

Thus, personal information will continue to be at risk due to security difficulties.

CONCLUDING REMARKS - A PARADIGM SHIFT IN DATA PRIVACY LAW?

The terms 'paradigm' and 'paradigm shift' have gained such a degree of popularity that they arguably have crossed the border separating meaningful terms from the land of meaningless clichés. Perhaps this overuse is sparked by an overemphasis, at least in the academic world, on works resulting in paradigm shifts - such works are frequently seen as the hallmark of great scholarship. However, one may wonder whether such an overemphasis may be disruptive and thereby harmful to academic work.

In any case, and at the risk of playing a part in what may be harmful behaviour, I suggest that there may be reasons to consider whether we are reaching a need for a paradigm shift in data privacy law resulting, in no small part, from the special characteristics of the Internet environment.

Without engaging with the highly interesting literature on the topic, it could perhaps be said that we are in a largely consent-

64 Australian Defence Signals Directorate http://www.asd.gov.au/publications/Information_Security_Manual_2014_Exec_ Companion.pdf, at 5.

based paradigm of informational self-determination. And the most interesting question is what type of paradigm we then are, and ought to be, moving towards. One possibility is that we are moving towards a paradigm of what in derogatory terms could be referred to as 'nanny state data protection'.

Despite the negative term, such an alternative may not be all bad, and inspiration could be drawn from the, now superseded, EU Council Directive on unfair terms in consumer contracts came into force on the 11th of May 1993.[65] Put simply, the structure of this Directive includes a set of broadly worded principles[66] that are backed up by a list of specific examples of conduct[67] that would typically violate those principles.

The approach taken in that Directive could be seen as a step away from party autonomy and self-determination in that it, whatever may be the genuine wishes of the parties, prevents certain types of contract terms from being included in certain types of contracts under certain conditions.

One can easily picture a similar 'nanny state' approach in data privacy law, which would mark a departure from a largely consent-based paradigm of informational self-determination. The advantages are obvious. For example, if the rules in question are carefully drafted, they may provide a clearer guidance for businesses and other organisations handling personal data. Further, and most importantly, we would no longer need to rely on the fairy-tale like notion of 'genuine consent'[68]- a notion that even if we all can describe it, we all know does not exist in reality.

BIBLIOGRAPHY

Adrian, Angelka (2013) 'How Much Privacy Do Clouds Provide? An Australian Perspective' (2013) 29 Computer Law and Security Review 48, 56 stating, 'Younger generations have much less concern about online privacy than older generations.

Australian Law Reform Commission, Unfair Publication: Defamation and Privacy, Report No. 11 (1979).

65 See Council Directive 93/13/EEC of 5 April 1993.

66 For example Article 3(1): "A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."

67 For example Annex 1: "Terms which have the object or effect of: (a) excluding or limiting the legal liability of a seller or supplier in the event of the death of a consumer or personal injury to the latter resulting from an act or omission of that seller or supplier;".

68 For consent to be viewed as being genuine, it needs to (1) be given freely, (2) be sufficiently informed and (3) be identifiable.

Dan_Svantesson@bond.edu.au

Australian Defence Signals Directorate http://www.asd.gov.au/publications/Information_Security_Manual_2014_Exec_Companion.pdf,

Bagaric, Mirko (2007) 'Privacy Is the Last Thing We Need', The Age (online), (22 April 2007) <http://www.theage.com.au/news/opinion/privacy-is-the-last-thing-we-need/2007/04/21/1176697146936.html>.

Bagaric, Mirko (2013) 'Rights Must Yield to Community Prosperity: The Fallacy That Is a Strong Right to Privacy' in Brett Mason and Daniel Wood (eds), Future Proofing Australia : The Right Answers for Our Future (Melbourne University Press, 2013)

Bygrave, Lee A (2014) Data privacy law: An international perspective (Oxford, Oxford University Press), xxv.

Brandeis, Louis and Warren, Samuel (1890) 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 195 (footnotes omitted).

Bygrave, Lee A. (2014)Data privacy law: An international perspective (Oxford, Oxford University Press, 2014).

Christopher, (2008) The 'Internal Morality' of European Data Protection Law (November 24, 2008). Available at SSRN: http://ssrn.com/abstract=1443797 or http://dx.doi.org/10.2139/ssrn.1443797,

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No 108 (adopted on 28 January 1981).

Cate, Fred H (1998)'The European Data Protection Directive and European-US Trade' (1998) 7 Currents: International Trade Law Journal 61, 73. While now slightly dated, this article provides an interesting comparison between US and EU data privacy law. See also, eg: Steven R Salbu, 'The Datalag (Sweden) 1973:289.

Data Protection Commissioner, (2007) Section 1: What is Privacy? (14 November 2007) <http://www.dataprotection.ie/documents/204teens/cspe%20resource%20booklet/Section_2_-_Privacy_as_a_ Human_Right.pdf>.

European Union Data Privacy Directive and International Relations' (2002) 35 Vanderbilt Journal of Transnational Law 655. Directive 95/46/EC of the European Parliament and of the Council 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.

European Commission, (2011) Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union (June 2011) <http://ec.europa.eu/public_opinion/archives/ ebs/ ebs_359_en.pdf> 1-3.

Hon, W Kuan and Millard, Christopher (2012), 'Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4' (2012) 9:1(25) SCRIPT-ed 8 [Queen Mary School of Law Legal Studies Research Paper No. 85/2011] <http://dx.doi.org/10.2139/ssrn.1925066>.

Gleick, James, 'Big Brother Is Us', The New York Times, 29 September 1996 <http://www.nytimes.com/1996/09/29/magazine/ big-brother-is-us.html?pagewanted=all&src=pm>.

Mark Burdon and Paul Telford, The conceptual basis of personal information in Australian privacy law, eLaw Journal: Murdoch University Electronic Journal of Law (2010) 17(1).

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Case C-131/12).

Graham Greenleaf, (2912)'The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108' (2012) 2(2) International Data Privacy Law 68, 72.
o Graham Greenleaf and Nigel Waters, (2012) 'Obama's Privacy Framework: An Offer to Be Left on the Table?' (2012) 119 Privacy Laws and Business International Report 6-9.

Harris, Edward C (2006-2007) 'Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers' (2006-2007) 22 American University International Law Review 746.

Harris, Edward C (2006-2007)'Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers' (2006-2007) 22 American University International Law Review 746, 746.

This discussion draws upon: Dan Svantesson, Fundamental policy considerations for the regulation of Internet cross-border privacy issues, Policy & Internet Vol. 3(3) 2011, Article 7 (2011).

International Covenant on Civil and Political Rights, GA Res 2200A (XXI), 21 UN GAOR Supp No 16, UN Doc A/6316/1966, 999 UNTS 171 (entered into force 23 March 1976), art 17 ('ICCPR') and the

Dan_Svantesson@bond.edu.au

Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), as amended by Protocols No 11 and No 14 (Rome, 4.XI.1950) ('ECHR').

Kuner , Christopher et al, (2012) 'Moving Forward Together' (2012) 2(3) International Data Privacy Law 81.

Kuner Christopher et al, (2012)'Editorial: The Challenge of "Big Data" for Data Protection' (2012) 2 (2) International Data Privacy Law

Information Wants to Be Free (7 May 2013) Wikipedia <http://en.wikipedia.org/wiki/Information_wants_to_be_free>.

Ministry of Internal Affairs and Communications (Japan), (2010) White Paper on Information and Communications in Japan 2010 <http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2010/2010-index.html>.

Moshell, Ryan (2004-2005) '...And Then There Was One: The Outlook for a Self-Regulatory United States amidst a Global Trend toward Comprehensive Data Protection' (2004-2005) 37 Texas Tech Law Review 357, 366.

Nygh, P and Butt, P (1998) Butterworths Concise Australian Legal Dictionary (2nd edn, Sydney, Butterworths,)

Olivecrona, Karl (1962) Legal Language and Reality, in Essays in Jurisprudence in Honor of Roscoe Pound. Ed. R. A. Newman, 151-91. Indianapolis, IN: Bobbs-Merrill. 1962.

Post, R.C. (2001) Three concepts of privacy, 89(6) Georgetown Law Journal 2087.

Poullet, Yves (2007)'Transborder Data Flows and Extraterritoriality: The European Position' (2007) 2(3) Journal of International Commercial Law and Technology 141, 143 (footnote omitted).

(2000/C 364/01). The Charter only came into force 1 December 2009.206

Rubinstein, Ira S (2013)'Big Data: The End of Privacy or a New Beginning?' (2013) 3 (2) International Data Privacy Law 74, 74.

Suszek, Mike (2013) Sony DropsAppeal for ICO-Issued 2011 Data Loss Fine (13 July 2013) Joystick <http://www.joystiq. com/2013/07/13/sony-drops-appeal-for-ico-issued-2011-data-loss-fine/>.

Shapiro, Fred R and Pearse, Michelle (2011-2012) 'The Most-Cited Law Review Articles of All Time' (2011-2012) 110 Michigan Law Review 1483, 1489.

Schwartz, John (2001)'As Big PC Brother Watches, Users Encounter Frustration', New York Times, 5 September 2001, C6.

Schneier, Bruce (2010) Google and Facebook's Privacy Illusion (4 June 2010) Forbes.com <http://www.forbes.com/2010/04/05/ google-facebook-twitter-technology-security-10-privacy. html?boxes=Homepagechannels>.

Svantesson, Dan and Clarke, Roger (2010) 'Privacy and Consumer Risks in Cloud Computing' (July 2010) 26(4) Computer Law and Security Review 391-7.

Sullivan, Clare (2014) Protecting digital identity in the cloud: Regulating cross border data disclosure (2014) 30(2) Computer Law and Security Review 137-152, at 152.

Tate, Ryan (2009)'Google CEO: Secrets Are for Filthy People' (4 December 2009) Gawker <http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people>. For a strong rebuttal of such claims, see: Daniel J Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745.

'The Nordic Youth IGF conference (NYIGF) was a pre conference to EuroDIG. Thirty youths in the age group of 14 - 17 years from Norway, Denmark, Iceland, Finland and Sweden formed the Nordic Youth Delegation. The NYIGF youth conference resulted in a number of recommendations regarding Internet governance': European Dialogue on Internet Governance Secretariat (EuroDIG), Messages from Stockholm (14-15 June 2012) <http://www.guarder. net/eurodig/2012/EuroDIG%202012_short_messages_to%20 the%20IGF_final.pdf>

Viviane Reding, 'The European Data Protection Framework for the Twenty-First Century' (2012) 2(3) International Data Privacy Law 119, 129. Importantly, Reding's assertion as to the competitive advantages to be gained from a well-structured data privacy framework has also been recognised by industry. See, eg: Peter Cullen and Jean Gonié, '1995 - 2012: from a Directive to a Regulation, the Microsoft Perspective' (2012) 2(3) International Data Privacy Law 117, 117.

Warren, S and Brandeis, L. (1980) The Right to Privacy, 4 Harvard Law Review 193.

Dan_Svantesson@bond.edu.au