1-1-2011

Fundamental policy considerations for the regulation of Internet cross-border privacy issues

Dan J.B. Svantesson
Bond University, dan_svantesson@bond.edu.au

Policy & Internet
www.policyandinternet.org

Volume 3, Issue 3 • 2011 • Article 7

Fundamental Policy Considerations for the Regulation of Internet Cross-Border Privacy Issues

Dan J.B. Svantesson, ***Bond University***

Svantesson, Dan J.B. (2011) "Fundamental Policy Considerations for the Regulation of Internet Cross-Border Privacy Issues," *Policy & Internet*: Vol. 3: Iss. 3, Article 7.
Available at: http://www.psocommons.org/policyandinternet/vol3/iss3/art7
DOI: 10.2202/1944-2866.1138

Fundamental Policy Considerations for the Regulation of Internet Cross-Border Privacy Issues

Dan J.B. Svantesson, ***Bond University***

Abstract

We are currently witnessing major changes to the regulation of privacy, both in Europe and North America, as well as in the Asia-Pacific region. One of the most complex and controversial aspects of any regulatory scheme addressing privacy is the regulation of cross-border data flows, and such regulation has become all the more complex in an interconnected world. After providing some necessary background observations regarding the issues surrounding the regulation of cross-border data flows on the Internet, this article identifies and analyses eight fundamental policy considerations for any regulatory scheme addressing cross-border privacy issues.

KEYWORDS: privacy, law, policy, Internet

Author Notes: Associate Professor, Faculty of Law Bond University, Gold Coast Queensland 4229 Australia, Tel: +61 7 5595 1418, Email: Dan_Svantesson@bond.edu.au, (www.svantesson.org). This article was finished during the author's time as a Visiting Academic at the Oxford Internet Institute (Oxford, England) March 2011. It is based on a Working Paper written during the author's time as a Visiting Fellow at the European University Institute (Florence, Italy) in February 2010. The author wishes to thank all the friendly staff members at the OII and the EUI, as well as the following people for their valuable input on the Working Paper: Professor Ross Buckley, Dr Lee Bygrave, Professor John Farrar, Mr Christopher Kuner, Dr Radim Polčák, Professor Giovanni Sartor and Professor William Van Caenegem. The views expressed are those of the author alone.

Introduction

We are currently witnessing major changes to the regulation of privacy, both in Europe and in North America, as well as in the Asia-Pacific region. One of the most complex and controversial aspects of any regulatory scheme addressing privacy, and more specifically the sub-section of privacy law known as data protection, is the regulation of cross-border data flows. Such regulation has become all the more complex in our interconnected world. After providing necessary background observations regarding issues surrounding the regulation of cross-border data flows on the Internet, this article identifies and analyzes eight fundamental policy considerations for such regulation. These policy considerations ought to be kept in mind for any regulatory scheme that addresses cross-border data flows on the Internet.

Background

The development of privacy as a legal concept, and the important functions that concept fills, have been well documented elsewhere, and will not be repeated here.[1] For the purpose of this article, it suffices to note that, despite its relatively lengthy history, and despite being a globally recognized fundamental human right, on a practical level privacy is not deeply rooted in the minds of the public. Instead, one frequently comes across the attitude that only those who are seeking to hide something are interested in privacy; or the corollary: "if you have nothing to hide, why worry about privacy?"

As is convincingly argued by Solove (2007, 745), such views are mistaken. Further, they are particularly worrying when expressed by people who are in a position to seriously affect the privacy protection afforded to the public. For example, it is disappointing to see Google's (now former) CEO Eric Schmidt state that: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (Tate 2009). Even worse, Facebook's Chief Executive, Mark Zuckerberg, has declared the age of privacy to be over (Schneier 2010). The significance of this type of attitude is emphasized by the fact that "technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive" (*United States v. Garcia* 2007, 998). In some cases, individuals are blissfully unaware of their privacy being violated, but in other cases individuals are knowingly and willingly sacrificing their privacy for the convenience of access to information technology resources:

[1] There is a wealth of high quality literature on the topic. Some examples are Warren and Brandeis (1890), Bygrave (2002), Swire and Litan (1998), Larremore (1912), Solove (2007), Gunasekara (2007), Reidenberg (2000), and Chik (2006).

> "As consumers and as citizens, we repeatedly trade convenience for control, handing over growing amounts of information about ourselves to others in the process. Our lives are increasingly mediated by digital technologies and described by data held in digital formats. We are racing ahead quickly with the development of new technologies while the institutions—legal and otherwise—designed to protect user privacy have lagged behind. The tradeoffs involved are rarely conscious ones." (Palfrey 2008, 243)

Palfrey goes on to note that "this growing problem has its roots in the fact that, as information technologies improve in efficiency and become more integrated in everyday life, fewer and fewer citizens are likely to know what information is being collected about them and by whom" (Palfrey 2008, 243). While this certainly is true, the problem also has another cause, as exemplified in the recent developments of covert tracking and surveillance facilities for mobile phones (Wolf 2010). Those involved in designing technologies frequently fail to assess the societal implications of the use of the products they develop (Cressman 2010). To address this, technology developers must take account of the fact that not everything technically "doable" should be done.

Schartum (2010, 1) describes how data protection is being impaired by three major factors:

> "i) changing statutory content as a result of a shift in the balance of interests, ii) inadequate formulation of data protection laws, and iii) insufficient ability to implement and enforce such laws. Factor i) refers to a re-evaluation of data protection in relation to other values and interests (cf. anti-terror measures, organised crime, health services etc.), and concerns mainly the political level. Factor ii) refers to how and where political intentions are placed and expressed in legal instruments (directives, national legislation, etc.), while factor iii) encompasses issues of awareness, communication and interpretation of data protection laws."

In the context of societal attitudes towards the right of privacy, it is interesting to look at that right from Olivecrona's perspective. Discussing the meaning (or lack thereof) of the terms "rights" and "duties," Olivecrona (1962, 183) has 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."

DOI: 10.2202/1944-2866.1138

Applying this to privacy, the reality is that one person's right of privacy far too seldom results 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 often be amber: signaling the risks associated with an uncharted territory. Further, it seems that a large section of the younger generation simply ignore the lights altogether in their use of Facebook and other social media. In other words, people in general either have too vague an idea of what entitlements stem from their right of privacy, or fail to appreciate the importance of privacy, and the social, political, and economical value that is attached to their personal data.[2] At the same time, businesses, governments, 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—if we return to Olivecrona's terminology, it could be said that we need privacy rights to result in clearer green lights and clearer red lights.

This can be contrasted with other human rights; perhaps most beneficially with the right that most often competes directly with the right of privacy: the right of freedom of expression. When it comes to freedom of expression, most people perceive a very strong green light: indeed, in many cases a stronger green light than may be justified under the law. At least in most western countries, people feel they have a right to say whatever they want to say and, at the same time, most people perceive a strong red light preventing them from interfering with other people's right to free expression.

Turning to the issue of cross-border data flows more specifically, it is clear that, with advances in communication technologies, the branch of privacy law that focuses on data protection has grown in significance. Indeed, with more and more data being collected, by an increasing number of diverse entities, it can reasonably be expected that data protection will continue to increase in significance.

Cross-Border Data Flows

One of the most interesting and controversial areas of data protection, in our interconnected world, is the regulation of cross-border data flows. Regulation goes back at least to the Swedish Data Act of 1973. Section 11 of that Act makes

[2]The terms "personal data" and "personal information" are used interchangeably throughout this article. As to the social, political, and economical value of personal data, it has been noted that "in some sectors, particularly in the on-line environment, personal data has become the de facto currency in exchange for on-line content." Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, at 5, WP 173 (adopted on July 13, 2010), see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

it clear that: "If there is reason to assume that personal data will be used for automatic data processing abroad, the data may be disclosed only after permission from the Data Inspection Board [Datainspektionen]. Such permission may be given only if it may be assumed that the disclosure of the data will not involve undue encroachment upon personal privacy" (Datalag 1973, 289 11 §). Furthermore, a later amendment to the Act (Datalag 1973, 7 a §) makes it clear that: "The responsible keeper of a file shall have in his possession an up-to-date list of the personal files for which he is responsible. The list shall contain particulars of … the extent to which personal data are disseminated for automatic data processing abroad."[3]

In his comprehensive work dealing with privacy regulation, Bygrave (2002) discusses the rationale of cross-border data flow regulations: "The chief aim of these rules is to hinder data controllers from avoiding the requirements of data protection laws by shifting their data-processing operations to countries with more lenient requirements (so-called 'data havens')." So far, this aspect of privacy law has gained relatively limited academic attention (but see, for example, Kuner 2010). However, with an ever-increasing degree of globalization, there are reasons to think that the attention afforded to this issue will increase.

This article identifies eight fundamental policy considerations for the regulation of cross-border data flows on the Internet. These are:

- People have a basic, but limited, right of privacy.
- People have a basic, but limited, right of freedom of expression.
- Modern society requires cross-border transfers of some data.
- Some of this data is personal in nature.
- Data crossing borders represents a loss of control for the data subject.
- Not all technologies are set up to be sensitive to data crossing borders.
- The regulation of cross-border data flows must be technology neutral.
- Effective protection of privacy is dependent on a widespread understanding of the right of privacy.

Any attempt to regulate cross-border data flows on the Internet must take into account all eight of these policy considerations. Each will now be analyzed in detail.[4]

[3]Swedish translations verified by the author.

[4]It must be noted that, while these policy considerations impact directly on the issue of cross-border data flows, they may also have wider implications on privacy more generally, and therefore be of broader interest.

DOI: 10.2202/1944-2866.1138

1. People Have a Basic, But Limited, Right of Privacy

The jurisdictional scope of the right of privacy is typically discussed in the context of instruments such as the Organisation for Economic Cooperation (OECD)'s Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Occasionally, one also sees this issue discussed by reference to established jurisdictional principles under international law (most notably the "territoriality principle"; Toy 2010). However, an examination of the jurisdictional scope of the right of privacy could also take as its point of departure the fact that privacy is a fundamental human right recognized in several international instruments, such as the United Nation's International Covenant on Civil and Political Rights (ICCPR) of 1966.[5] More specifically, Article 17 of the ICCPR states that:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks."

As privacy is at the heart of the current inquiry, identifying this right and its scope is of great importance—there can be no doubt that this right constitutes a fundamental policy consideration for any regulatory scheme addressing cross-border data flows on the Internet.

The problem is, of course, that, so far, there have been no successful attempts at defining the scope of this right with any great precision. That is, the question "What is privacy?" does not have an obvious or universally accepted answer. In the simplest sense, privacy could be said to mean the "right to be let alone" (Warren and Brandeis 1890). Another possible definition is that privacy is "the interest of a person in sheltering his or her life from unwanted interference or public scrutiny" (Nygh and Butt 1998). A more sophisticated definition would be to say that privacy relates to "material that so closely pertains to a person to his innermost thoughts, actions and relationships that he may legitimately claim the prerogative of deciding whether, with whom and under what circumstances he will share it" (Australian Law Reform Commission 1979). Neither of these definitions could be said to be more correct than the others, but taken together they provide a relatively clear sense of what we mean when we talk about privacy.

[5] The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty adopted by the United Nations General Assembly. Part of the International Bill of Human Rights, it entered into force on March 23, 1976 and has so far been ratified by 167 state parties.

Perhaps the most interesting question, in terms of the scope of the right of privacy, is its jurisdictional limitations. The simple fact is that, for a person's privacy to be adequately protected, it must be protected against abuse regardless of the geographical source of that abuse. It is not sufficient to be protected against abuse by individuals and organizations in one's own jurisdiction, if those located outside it can collect, use, and distribute one's personal information in contravention of one's right of privacy.

To understand how Article 17 is meant to work in a cross-border context, we must take into account Article 2(1) of the ICCPR:

> "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."

It seems possible to argue that the phrase "to respect and to ensure to all individuals *within its territory and subject to its jurisdiction* the rights recognized in the present Covenant" (author emphasis) expresses two separate requirements rather than a double requirement (Joseph et al. 2000; Nowak 1993). From that vantage point, Article 17 means that each signatory state has an obligation to provide legal protection against unlawful attacks on the privacy of people subject to its jurisdiction *and* those present within its territory, regardless of the origins of the attacks.

While potentially controversial under the rules of jurisdiction under international law, this interpretation is supported in ICCPR General Comment 16: "Provision must also be made for everyone effectively to be able to protect himself against *any* unlawful attacks that do occur and to have *an effective remedy* against those responsible" (author emphasis; Human Rights Committee 1988). If the privacy of a person in state B is negatively affected by material originating in state A, state B is arguably failing to provide "an effective remedy against those responsible" unless its laws provide for jurisdictional and legislative claims over the offender in state A.[6] In other words, Article 17(2) of the ICCPR appears to be a source of international law, requiring signatory states to make fairly wide jurisdictional claims in relation to the protection of the privacy of people within their jurisdiction or territory.

[6] It can, of course, be said that even such a jurisdictional claim does not in itself provide "an effective remedy against those responsible" unless it can also be enforced. However, state B in our example cannot be required to do more than what is in its power to do.

DOI: 10.2202/1944-2866.1138

2. People Have a Basic, But Limited, Right of Freedom of Expression

Like the right of privacy, the right of freedom of expression is a basic human right. Article 19 of the ICCPR provides that everyone shall have the right to hold opinions without interference:

> "1. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> 2. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order (ordre public), or of public health or morals."

The right of freedom of expression has also, directly or indirectly, made its way into many countries' fundamental laws. The most obvious example is the First Amendment to the U.S. Constitution, which states that: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." Other countries do not so clearly proclaim this right. In Australia, for example, the High Court has, in the absence of express provisions in the Constitution, recognized an implied right of free political speech.[7] Other countries include freedom of speech in their fundamental law without applying it in a manner that provides for an effective protection of free speech. For example, Article 35 of the 1982 Constitution of the People's Republic of China states that: "Citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession and of demonstration." Either way, this article only considers freedom of expression from the perspective of how it works under the ICCPR.

As with the right of privacy, in order to assess the implications of the right of freedom of expression for cross-border data flows, it is necessary to examine its jurisdictional scope: while it is clear that there is a right of freedom of

[7] Refer to the landmark cases of *Nationwide News Pty Ltd v. Wills* (1992) 175 C.L.R. 1 (Austl.); *Australian Capital Television Pty Ltd v. The Commonwealth* (1992) 175 C.L.R. 106.

expression, we must ask whether this right can cross borders. To assess the jurisdictional scope, it is necessary to return to ICCPR Article 2(1) (above). It makes clear that State Parties to the ICCPR undertake to respect and to ensure "to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant." Imagine that a person in state A places content on a website, and as a result is prosecuted in state B. State B can only do so successfully if it regards itself to have jurisdiction, under its domestic rules of private international law, over the offender in state A. In that case, state B should reasonably also view itself as having jurisdiction for the purposes of Article 2(1) of the ICCPR, with the consequence that state B must respect the offender's right of freedom of expression. It therefore seems clear that, like the right of privacy, the right of freedom of expression can cross borders. Any other conclusion would mean that freedom of expression does not apply when using Internet technologies with a global reach—a disturbing outcome indeed.

It is, however, necessary to distinguish between situations where a state is applying its laws in a manner that restricts people in other states from exercising their freedom of expression on the one hand, and situations where a state applies its laws in a manner that allows free expression within its borders, but does not allow the expression to cross its borders. The first type of situation would, for example, arise where a person in state A places content on a website, and as a result is prosecuted in state B. The second type of situation would arise, for example, where special rules regulate cross-border data flows: a person has the freedom to express themselves within the borders of the state, but not where the expression represents the export of personal data.[8]

While the first of these situations would represent a violation of the freedom of expression, the status of the latter is less certain.

3. Modern Society Requires Cross-Border Transfers of Some Data

Possibly the easiest way to avoid privacy violations arising from personal data crossing borders would be to disallow such transfers. However, such an approach is utterly incompatible with the needs of modern society (Blume 2006), given the diverse activities—such as commerce, law enforcement, and even some aspects of healthcare—that require cross-border data flows. Further, modern technologies

[8] Care must, however, be taken in determining the circumstances in which such restrictions may be placed on the freedom of expression. This is particularly so bearing in mind the important role cross-border information flows may play for human rights developments in places where such developments are most needed. See Koutouki (1999) and Husain (2008).

DOI: 10.2202/1944-2866.1138

like the Internet would simply not work in the absence of such transfers. Restrictions on cross-border data transfers may often be an impediment to cross-border e-commerce and other valuable international interactions, such as social networking.

In light of this, a fundamental policy consideration for any regulatory scheme that addresses cross-border data flows on the Internet is that it must allow such data flows so as to not unduly restrict or limit the proper function of Internet communication. Further, while not all forms of personal information must cross borders in all imaginable situations, the regulation must not restrict such data flows unless such restriction is necessary.

4. Some of the Data that Necessarily Crosses Borders for the Proper Function of Internet Communication is Personal in Nature

Privacy laws will typically only protect information that is personal. Consequently, to determine whether a particular instance of cross-border data transfer amounts to a privacy concern under current laws, it is necessary to establish whether the information, or data, in question falls within the definition of "personal information" or "personal data." This brings us to the actual definition of "personal information" or "personal data," which, as can be expected, varies between jurisdictions. Despite the diversity, certain general observations can be made. For example, the OECD and Asia-Pacific Economic Cooperation (APEC) both define personal information/data to mean any information about or regarding an identified or identifiable individual (OECD 1980, Part 1; APEC 2004).

The European Union's definition, as well as the definition found in the Australian Privacy Act 1988 (Cth), is more detailed:

> "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." (EU Directive 95/46, Article 2a)

> "'personal information' means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." (Australian Privacy Act 1988 (Cth), s. 6)

Studying these provisions, there can be little doubt that if, for example, a medical practitioner in one country exports identifiable patient data to a medical practitioner (or drug company) in another country, that will amount to a transfer of personal data. Similarly, where a company in state A collects data relating to the shopping habits of its consumers in state A, and then transfers that data to another company in state B, we have a case of transfer of personal data. This is uncontroversial and needs no further discussion. But there are important borderline cases, and more interesting questions arise if we ask whether the type of data that is necessarily transferred across borders, as part of the Internet's basic operation, meets the test of constituting personal data. For example, is an email address (e.g., dasvante@bond.edu.au) personal information? Can an Internet Protocol (IP) address (e.g., 131.244.15.161) amount to personal information? These matters have gained considerable attention in recent years, and it is necessary to discuss email addresses and IP addresses separately.

There are several factors that affect whether an email address can amount to personal data. For example, there is a difference between addresses that include a person's name (e.g., John_Lennon@bond.edu.au or john@lennon.org) and addresses that provide no clear identity clues (e.g., asdfghj1234@hotmail.com). It is of course more likely that the former type can be viewed as being personal data than the latter. Furthermore, there is a difference between email addresses that reveal an organization (e.g., @eui.eu) and more generic ones (e.g., @gmail.com). In a similar manner, email addresses that indicate a specific geographical region (e.g., @qld.gov.au) may be more likely to amount to personal data. The underlying consideration is whether the email address as a whole, combined with any other accessible data, reasonably identifies a person (whether correctly or incorrectly) as being the data subject.

These considerations are also valid for IP addresses; however, they are typically more complicated. Several cases from various jurisdictions have considered this issue. In some cases, the court has decided that IP addresses are not personal in nature. For example, in the U.S. case *Columbia Pictures Indus. v. Bunnell* (2007) the court stated that: "As an IP address identifies a computer, rather than a specific user of a computer, it is not clear that IP addresses […] are encompassed by the term 'personal information' in defendants' website's privacy policy." Other U.S. courts have reached virtually identical conclusions.[9] Similarly, in Hong Kong (SAR) the Administrative Appeals Board has upheld the Hong Kong Privacy Commissioner's view that an IP address does not per se satisfy the definition of personal data, since it is "information about an inanimate computer, not an individual" (*Shi Tao v. The Privacy Comm'r For Pers. Data* 2007).

[9] See *Johnson v. Microsoft* (2009).

DOI: 10.2202/1944-2866.1138

In contrast, the EU's Article 29 Data Protection Working Party[10] takes the view that "IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66" (Opinion 2/2002). The Working Party reached its conclusion in light of the fact that "in the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means" (Opinion 2/2002).

Interestingly, there is a diversity of opinion among the EU member states: the Appeal Court of Paris has ruled in several judgments that an IP address only allows one to identify a computer, and, therefore, its processing does not allow one to identify its user (Coudert and Werkers 2010). While there no doubt may be strong political reasons motivating such a conclusion, such as the impact this interpretation has in relation to copyright societies,[11] the view I would favor was expressed by a Swedish administrative court, StockholmsLänsrätt, in 2006. The case arose from the actions of Antipiratbyrån—a private organization aiming to identify file sharers and bring them to prosecution—who had collected data, including IP addresses, for this purpose. It was undisputed in the case that ISPs can identify subscribers based on the IP address, but the Antipiratbyrån argued that, as the user could be a person other than the subscriber, the IP address is not personal information. The court did not agree. The majority held that: "The physical person that can be identified by reference to the IP number need not be the actual user. Rather, already the fact that a physical person can be identified as the subscriber is sufficient for the IP number to be regarded as personal information under PUL ['Personuppgiftslagen' i.e., the relevant Act]."[12] The view expressed by the Stockhomcourt is therefore in line with the approach taken by the Article 29 Data Protection Working Party.

The Australian Law Reform Commission took a position representing a form of middle ground. It stated that: "Information that simply allows an individual to be contacted—such as a telephone number, a street address or an IP address in isolation—would not fall within the recommended definition of 'personal information'" (Australian Law Reform Commission 2008, 6.61). However, it also stated that:

> "While stand alone telephone numbers, street addresses and IP addresses may not be personal information for the purposes of the *Privacy Act*, such

[10] The Article 29 Data Protection Working Party was established by Article 29 of Directive 95/46/EC as an independent EU Advisory Body on Data Protection and Privacy.

[11] I stress that I am here not suggesting that such political considerations unduly influenced the French court.

[12] Case number 15646-05 (decided 2006) of the StockhomLänsrätt (author's translation).

> information may become personal information in certain circumstances. The ALRC acknowledges that telephone numbers relate to telephones or other communications devices, IP addresses to computers, and street addresses to houses, rather than individuals, but notes that such information may come to be associated with a particular individual as information accretes around the number or address." (Australian Law Reform Commission 2008, 6.60)

In light of the above, it is no wonder that commentators conclude that the debate is still open as to whether IP addresses amount to personal information (Coudert and Werkers 2010, 60). However, perhaps it can be concluded that in some instances IP addresses are highly likely to be widely recognized as personal information, that in other instances they are unlikely to be so recognized, and that this will vary from jurisdiction to jurisdiction, and possibly from court to court. In summary, there can be no doubt that both email addresses and IP addresses can amount to personal information in some circumstances.

5. Data Crossing Borders Represents a Loss of Control for the Data Subject

A fundamental policy consideration is found in the fact that once data crosses borders, the data subject loses a degree of control over the data (Blume 2006, 22). While this proposition may be rather self-evident, it is nevertheless necessary to expand on what is meant by "control" in this context.

I am not primarily referring to any actual ability to influence how an organization uses or discloses our personal data. The reality is that, once data is in the hands of an organization, data subjects have no actual control over its use and the disclosure of the data; such is the nature of information. Instead, what is being referred to here as "control" has, at least, four aspects:

- The ability to detect misuse
- The ability to identify the party responsible for the misuse
- The ability to hold that party accountable for the misuse
- The ability to prevent further misuse by that party

Thus, "control" in this context relates to retroactivity rather than prevention, and all four aspects of control are typically negatively affected through cross-border data transfers. While it is possible to imagine exceptions, in most cases it is harder to detect misuse overseas, and harder to identify the party responsible. Further, holding a party located overseas accountable is typically

DOI: 10.2202/1944-2866.1138

more difficult. First, once the responsible party has been identified, it may be hard to physically locate that party. Second, once identified and located, holding that party accountable involves finding an appropriate forum in which to seek redress, and establishing a liability under the applicable law. Third, the victim is often faced with severe enforcement difficulties. Finally, once data has been misused overseas, it may be more difficult to ensure that the data is not misused there in the future.

6. Not All Technologies are Set Up To Be Sensitive to Data Crossing Borders

The Internet was designed with certain requirements in mind. Most importantly for our purposes, the Internet was designed to allow for seamless data transfer across geographical borders: indeed, most communications occur without the persons involved in the communication being aware of the exact extent to which their communications cross any borders. For example, users are typically unaware of, and uninterested in, where their data is stored when they use cloud computing solutions such as some email services (e.g., Hotmail) and social networking tools (e.g., Facebook).

However, this is not the full story. Some countries have chosen to exercise a degree of border control. For example, the Internet in the People's Republic of China (PRC) is structured according to a four-tier system not dissimilar to that of many other states. Starting from the bottom we have the individual Internet users (tier four) who connect to the Internet through Internet Service Providers (ISPs) (tier three). The ISPs connect to an Internet Access Provider (IAP). The IAPs, representing the second tier, are the ones that actually own the physical networks, which are leased by ISPs. Finally the IAPs connect to the Government's gateway (tier one) and can thereby access the global Internet. What makes the PRC's system different from that of many other states is that it is prescribed by law.[13] Thus, for example, an Internet user may not connect to the Internet via a foreign ISP in order to circumvent the system.[14]

In contrast, most other countries cannot exercise any effective border control due to the fact that Internet communications, both domestic and foreign, go through a multitude of private and public carriers—there simply are no effective "strangle points." With this in mind, the "international Internet" can be

[13]See Provisional Regulation (1997). I have been unable to confirm whether this Provisional Regulation still is in force. However, the key point, that the PRC exercises a relatively strict control over what crosses its borders, is beyond doubt. See also ONI (2006).

[14] Any such attempts will be punished. See, for example, the Supreme People's Procuratorate (2002).

viewed as borderless, while, for example, the domestic sub-Internet in the PRC is borderless only within China, but not in relation to the rest of the world.

7. The Regulation of Cross-Border Data Flows Must Be Technology Neutral[15]

Researchers in the field of information technology law must always consider whether their findings are technology neutral or technology specific. Regulation is technology specific where it expressly, or implicitly, specifies the type of technology it applies to (as opposed to being applicable to any technology). The New Zealand Law Commission describes the need for "technological neutrality" in the following manner: "Technology has advanced with great speed in recent years. It is likely to continue to do so. Unlike technology, the law tends to develop slowly, usually by reacting to situations only as they arise. It is therefore vital that any reform of the law be drafted so as to take account not only of the technology currently available, but also that which has yet to be developed" (New Zealand Law Commission 1998).

The aims of technological neutrality, and the related concept of functional equivalence,[16] could be seen as extensions of a more general goal applicable to any form of regulation; that is, all laws must be drafted at a suitable level of abstraction. In other words, laws must aim to be applicable where such application is desirable, but not applicable where application is undesirable. Despite this foundation in an undisputable goal of legal drafting, and despite the fact that functional equivalence and technological neutrality have become widespread guiding principles for how legal drafters approach Internet regulation, the two concepts have not been free of criticism.

In an interesting article, Escudero-Pascual and Hosein demonstrate the potential downside of technology-neutral solutions: "a reason for technology-neutrality is to ensure that new laws do not need to be passed every time a new technology is invented. However, technology-neutral language may be used to ignore, wilful or not, the challenges, risks, and costs to applying powers to different infrastructures" (Escudero-Pascual and Hosein 2004). In other words,

[15]This section draws on Svantesson (2008).

[16] "The functional equivalence approach … is based on an analysis of the purposes and functions of the traditional paper based requirement with a view to determining how those purposes or functions could be fulfilled through electronic commerce techniques. … the adoption of the functional-equivalent approach should not result in imposing on the users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment." UNCITRAL (1996) Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998 at 20-21, U.N. Sales No. E.99.V.4.

DOI: 10.2202/1944-2866.1138

today's technology-neutral solution is not guaranteed to be a suitable form of regulation in relation to a future technology. Imagine the work on an Internet-related international convention, perhaps having lasted for ten years or more, producing a technology-specific text. If such a convention were completed in the late 1980s or early 1990s, it would presumably have addressed, for example, Bulletin Board System (BBS) communication, but certainly not World Wide Web (WWW) communication.[17] Keeping in mind the current high speed of technical development, and the slow legislative process both domestically and internationally, it may be pointless to create Internet-related technology-specific law. At the same time, we must question what effect a technology-neutral rule constructed in the late 1980s or early 1990s to perhaps address a BBS-specific concern would have on the WWW or peer-to-peer communications in use today. Furthermore, we need not look far to find examples of serious consequences lying in store where there is an overreliance on technological neutrality. For years, copyright regulations around the world have failed to cope with the peculiarities of digital media, such as music and movies. In my view, their stubborn attachment to a principally technology-neutral regulation has effectively rendered the copyright law in a state of bankruptcy.

To conclude, in the drafting of legal rules one must balance the risk of those rules becoming outdated and thereby useless (which will, in turn, call for new rules to be constructed), and the risk of those rules being applicable in situations they are not suited for. Further, it is not always obvious how the concepts of functional equivalence and technological neutrality are to be applied successfully in relation to electronic communications (Svantesson 2008).

8. Effective Protection of Privacy is Dependent on a Widespread Understanding of the Right of Privacy

As has been discussed above in the context of Olivecrona's red light/green light approach to rights, privacy as a right suffers from a lack of public awareness. With some notable exceptions,[18] governments have done too little to promote the protection of, and the public's interest in, privacy. Furthermore, privacy advocates typically do not have access to the necessary resources to do anything but ensure a minimum of attention being reserved for this "ugly duckling" among the fundamental human rights.

If this is correct, we must move on to ask how we can achieve a clearer understanding and stronger respect for the right of privacy. Olivecrona's writings

[17]The reader will recall that the use of the WWW is largely a trend from the mid-1990s.

[18] Such as, for example, the proactive approach taken on several occasions by the Canadian Privacy Commissioner, Jennifer Stoddart.

can aid us 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 promisee 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 exposed to a sanction if he breaks his promise; his awareness of this fortifies the immediate psychological effect of the promise on him." (Olivecrona 1962, 180)

Olivecrona also notes that: "The green and red lights do not express any notions. They are signs which have a social function because people have been taught to react to them in certain ways" (Olivecrona 1962, 183). Combining 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*, that right. As expressed by Schartum, "it is clearly insufficient to fight for a particular level of formal protection (law in book) unless this is combined with efforts to ensure reasonable conformity with the law in action" (Schartum 2010). The solution would then seem to lie in changing the psychological reaction to privacy rights, and applying law more effectively and visibly.[19] Indeed, combined with public education, a more effective and visible application of the law to protect privacy may change the psychological reaction to privacy rights.[20]

In light of the low awareness of the right of privacy, I think it is necessary for regulation addressing cross-border data flows to emphasize the right of privacy for both the data subjects and the data handlers. This is becoming increasingly important in the light of so-called Web 2.0 culture, where the data handlers may be individuals with little or no knowledge of the applicable law.[21] Put differently, all aspects of data regulation, including the regulation of cross-border data, should aim to create a climate where data handlers (be they organizations, government, or individuals) instinctively recognize Olivecrona's "red light" when they step over the line of what is permissible under the law.

[19]Other scholars have also argued in favor of this combination, see Chik (2006).

[20] For an interesting discussion of the importance of proper reporting, see Greenleaf (2002a; 2002b; 2002c) and Gunasekara (2007, 392).

[21] In relation to privacy in the context of Web 2.0, see Roth (2010).

DOI: 10.2202/1944-2866.1138

Interaction of the Fundamental Policy Considerations

It is perhaps to be expected that some policy considerations discussed here will strengthen each other, while others will require careful balancing. No instances have been found here of policy considerations that strengthen each other, but two clashes that require attention are discussed below.

Privacy versus Freedom of Expression

Perhaps the most interesting and important clash of fundamental policy considerations is that between the right of freedom of expression and the right of privacy. As this article's scope is restricted to the regulation of cross-border data, it would seem that the right of privacy trumps the right of freedom of expression for our purposes. First, for a signatory to comply with its obligations under Article 17 of the ICCPR, it needs to protect all individuals *within its territory and subject to its jurisdiction*, regardless of whether the attack is a domestic one or one originating overseas. In contrast, it is arguable that there is no suggestion that a state would fail to comply with Article 19 unless it allows for cross-border communications—arguably, a state ensures its compliance with Article 19 as long as all individuals *within its territory and subject to its jurisdiction* have a freedom of expression within its territory and jurisdiction.

The above suggests that the right of protection against privacy invasions, *regardless of the geographical origins of the invasions*, is more clearly a part of international human rights law, than is the right of free expression *across borders*. In any case, it is immediately clear to the reader of ICCPR Article 19 that this right is not absolute. However, while it is clear that one person's right of freedom of expression may be restricted by reference to the protection of other people's right of reputation, no specific reference is made to such restrictions based on the protection of other people's right of privacy. This may be thought of as being odd when one considers that the right of privacy, like the right of reputation, is established in Article 17 of the ICCPR.

As odd as this may seem, the negative implications of this peculiarity are mitigated by the broad reference to the "rights of others." As will be recalled, Article 19(3) makes it clear that the freedom of expression may be restricted by necessary laws for the respect of rights of others: "The permissible limitations of protection of 'rights of others' is a catch all limitation, and is potentially very broad. The HRC [Human Rights Committee] has never commented on its outer limits. It is hoped that 'rights' refers to other human rights, though not necessarily those in the ICCPR" (Joseph et al. 2000). Thus, in light of this interpretation, the clash between the right of freedom of expression and the right of privacy is an example of what we can call a *solvable*, or *illusory*, clash—a solution can be

found that caters to both needs, as neither of these policy considerations is absolute.

Loss of Control versus the Needs of Modern Society and the Structure of Relevant Technologies

There is also a clash between, on the one hand, the fundamental policy consideration that there is a loss of control where data crosses borders, and, on the other hand, the fundamental policy consideration that cross-border data transfers are required by modern society and that not all technologies are sensitive to data crossing borders. This clash is, of course, significantly affected by, or indeed dependent on, another fundamental policy consideration; namely, the fact that some of the data that necessarily crosses borders for the proper functioning of Internet communication is personal in nature.

What we find in this case is an example of an *unsolvable* clash—a solution cannot be found that caters for both needs in their entirety. Whenever a researcher comes across such a situation, they must assess whether the fundamental policy considerations in question can be balanced against each other in a manner that allows for each of them to be met to a sufficient degree. The solution to this particular clash lies in allowing cross-border transfers, but at the same time placing some restrictions on the circumstances under which such transfers can take place, and possibly also restricting the types of data that can be transferred (i.e., treating different types of personal data differently). The difficulty with unsolvable clashes is that the researcher must constantly be aware that in catering for one constraint, they are simultaneously undermining the other, competing, constraint.

Conclusion

This article has identified and analyzed eight different fundamental policy considerations that are of such importance that any regulatory scheme addressing cross-border data flows on the Internet must take account of them. The article has also examined how these policy considerations interact, demonstrating that the complexities involved in regulating these data flows go beyond simply balancing privacy protection against freedom of data flows. At the same time, it is also clear that balancing these two goals represents the unescapable core question for any regulatory scheme addressing this issue. As several bodies worldwide are currently constructing and modernizing regulatory schemes that address cross-

DOI: 10.2202/1944-2866.1138

border data flows,[22] it is hoped that this article constitutes a timely reminder of the fundamental policy considerations that must be taken into account.

References

Article 29 Data Protection Working Party. 2002. "Opinion 2/2002 on the Use of Unique Identifiers in Telecommunication Terminal Equipments: The Example of IPv6." http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp58_en.pdf.

Article 29 Data Protection Working Party. 2010. "Opinion 3/2010 on the Principleof Accountability." http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

Asia-Pacific Economic Cooperation. 2004. "APEC Privacy Framework." http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

Australian Capital Television Pty Ltd v. The Commonwealth. 1992. 175 CLR 106.

Australian Law Reform Commission. 1979. *Unfair Publication: Defamation and Privacy Law*. Report no. 11.

Australian Law Reform Commission. 2008. *For Your Information: Australian Privacy Law and Practice*. Report no. 108.

Blume, Peter. 2006. Retlig Regulering af Internationale. Persondataoverførsler. DJØF Forlag, Denmark.

Bygrave, Lee A. 2002. *Data Protection Law—Approaching its Rationale, Logic and Limits*. London: Kluwer Law International.

Chik, Warren B. 2006. "The Lion, the Dragon and the Wardrobe Guarding theDoorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore—Two Differing Asian Approaches." *International Journal of Law and Information Technology* 14: 47.

Columbia Pictures Indus. v. Bunnell. 2007. C.D. Cal. (May 29, 2007).

Coudert, F., and E. Werkers. 2010. In the Aftermath of the Promusicae Case: How to Strike the Balance? Int'l J.L. & Info. Tech. 18 (1) 58.

[22] Refer, for example, to the review of relevant EU law (Reform of EU Data Protection law: EDPS calls on the European Commission to be ambitious in its approach (EDPS/10/8, April 29, 2010) http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/10/8), and the work carried out by APEC (News Release, APEC Secretariat, APEC launches new Cross-border Data Privacy Initiative (July 16, 2010) for more details, APEC, APEC Crossborder Privacy Enforcement Arrangement, CPEA).

Cressman, Jordan. 2010. "Does Mobile Spying Software Go Too Far With Latest Update?" http://www.i4u.com/article33515.html.

Data Act (1973) 289. Sweden.

Escudero-Pascual A., and I. Hosein. 2004. "The Hazards of Technology-Neutral Policy: Questioning Lawful Access to Traffic Data." *Communications of the ACM* 47 (3). http://doi.acm.org/10.1145/971617.971619.

EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Greenleaf, Graham. 2002a. "Reporting Privacy Complaints Pt 1: A Proposal for Systematic Reporting of Complaints in Asia-Pacific Jurisdictions." *Privacy Law and Policy Reporter* 9 (3): 41.

Greenleaf, Graham. 2002b. "Reporting Privacy Complaints Pt 2: A Proposal for Systematic Reporting of Complaints in Asia-Pacific Jurisdictions." *Privacy Law and Policy Reporter* 9 (4): 74.

Greenleaf, Graham. 2002c. "Reporting Privacy Complaints Pt 3: A Proposal for Systematic Reporting of Complaints in Asia-Pacific Jurisdictions." *Privacy Law and Policy Reporter* 9 (6): 111.

Gunasekara, Gehan. 2007. "The 'Final' Privacy Frontier? Regulating Trans-Border Data Flows." *International Journal of Law and Information Technology* 15 (3): 362.

Human Rights Committee. 1988. "General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation." http://www2.ohchr.org/english/bodies/hrc/comments.htm.

Husain, Aisha. 2008. "Framing the International Standard on the Global Flow of Information on the Internet." *Interdisciplinary Journal of Human Rights Law* 3: 35.

International Covenant on Civil and Political Rights of 16 December 1966.

Johnson v. Microsoft. 2009. W.D.Wa. (June 23, 2009).

Joseph, S., et al. 2000. *The International Covenant on Civil and Political Rights: Cases Materials and Commentary*. New York: Oxford University Press.

Koutouki, Dina. 1999. "Human Rights: Benefits of Information Technology." *University of New Brunswick Law Journal* 48: 265.

Kuner, Christopher. 2010. "Data Protection Law and International Jurisdiction on the Internet (Part 1)." *International Journal of Law and Information Technology* 18 (176).

Larremore, Wilbur. 1912. "Law of Privacy." *Columbia Law Review* 12 (8): 694.

Nationwide News Pty Ltd v. Wills. 1992. 175 CLR 1.

New Zealand Law Commission. 1998. *Electronic Commerce Part One: A Guide for the Legal and Business Community*. Report 50.

DOI: 10.2202/1944-2866.1138

News Release, APEC Secretariat, APEC launches new Cross-border Data Privacy Initiative (July 16, 2010).

Nowak, M. 1993. *UN Covenant on Civil and Political Rights*. Germany, Kehl: N.P. Engel.

Nygh, Peter, and Peter Butt. 1998. *Butterworths Concise Australian Legal Dictionary*. Sydney: Australia.

Olivecrona, Karl. 1962. "Legal Language and Reality." In *Essays in Jurisprudence in Honour of Roscoe Pound*, ed. R.A. Newman. Indianapolis, Indiana: Bobbs-Merril.

OpenNet Initiative (ONI). 2006. "Internet Filtering in China in 2004–2005: A Country Study." http://www.opennetinitiative.net/studies/china/ (accessed April 25, 2006).

Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6.

Organisation for Economic Co-operation and Development. 1980. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html.

Palfrey, John. 2008. "The Public and the Private at the United States Border with Cyberspace." *Mississippi Law Journal* 78 (2): 241-292.

Privacy Act 1988 (Cth) Australia.

Provisional Regulations of the People's Republic of China for the Administration of International Connections to Computer Information Networks (1997).

Reform of EU Data Protection law: EDPS calls on the European Commission to be ambitious in its approach (EDPS/10/8, April 29, 2010) http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/10/8).

Reidenberg, Joel R. 2000. "Resolving Conflicting International Data Privacy Rules in Cyberspace." *Stanford Law Review* 52: 1315.

Roth, Paul. 2010. "Data Protection Meets Web 2.0: Two Ships Passing in the Night." *University of New South Wales Law Journal* 33: 532.

Schartum, Dag Wiese. 2010. "Designing and Formulating Data Protection Laws." *International Journal of Law and Information Technology* 18 (1): 1.

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

Shi Tao v. The Privacy Comm'r For Pers. Data. 2007. 16 Administrative Appeals Board 2007 (H.K.).

Solove, Daniel. 2007. "I've Got Nothing to Hide and Other Misunderstandings of Privacy." *San Diego Law Review* 44: 745.

Supreme People's Procuratorate. 2002. "Official Reply of the Supreme People's Procuratorate on the Application of Laws to Acts of Illegally Operating International, Hong Kong, Macao, or Taiwan Telecommunication Services." February 6, 2002. http://www.isinolaw.com.

Svantesson, Dan. 2008. "The Times They Are A-changing' (Every Six Months)—The Challenges of Regulating Developing Technologies." *Forum on Public Policy: A Journal of the Oxford Round Table.* http://forumonpublicpolicy.com/archivespring08/svantesson.pdf.

Swire, Peter, and Robert E. Litan. 1998. *None of your Business: World DataFlows, Electronic Commerce, and the European Privacy Directive*. Washington D.C: Brookings Institute Press.

Tate, Ryan. 2009. "Google CEO: Secrets Are for Filthy People." http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people.

Toy, Alan. 2010. "Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity." *New Zealand University Law Review* 24: 222.

UNCITRAL. 1996. Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998 at 20-21, U.N. Sales No. E.99.V.4.

United States v. Garcia. 2007. 474 F.3d 994, 998 (7th Circuit, 2007).

Warren S., and L. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4: 193.

Wolf, Jeffrey. 2010. "What Your Phone App Doesn't Say: It's Watching." http://www.9news.com/money/story.aspx?storyid=145727&catid=344.

DOI: 10.2202/1944-2866.1138