

Maurer School of Law: Indiana University

Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship

2013

The Extraterritoriality of Data Privacy Laws – An Explosive Issue Yet to Detonate

Fred H. Cate

Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner

Brussels Privacy Hub


Christopher Millard

Cloud Legal Project

Dan Jerker B. Svantesson

Bond University

Follow this and additional works at: <https://www.repository.law.indiana.edu/facpub>

 Part of the [Information Security Commons](#), [International Law Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Cate, Fred H.; Kuner, Christopher; Millard, Christopher; and Svantesson, Dan Jerker B., "The Extraterritoriality of Data Privacy Laws – An Explosive Issue Yet to Detonate" (2013). *Articles by Maurer Faculty*. 2622.

<https://www.repository.law.indiana.edu/facpub/2622>

This Editorial is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.



LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

Editorial

The extraterritoriality of data privacy laws—an explosive issue yet to detonate

Christopher Kuner*, Fred H. Cate**, Christopher Millard**, and Dan Jerker B. Svantesson***

Back in 1996, Rotenberg noted that: ‘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

This prophecy has largely been fulfilled. However, one aspect of data privacy law that has yet to gain the attention it deserves is the extraterritorial scope of data privacy laws. In a world so characterized by globalization, it is highly surprising that this issue has gained so little attention. Thus, our prophecy is that the extraterritorial application of data privacy laws will emerge more clearly as one of the most significant and urgent cross-border law questions over the coming years.

This point of view is supported by the fact that data privacy laws with extraterritorial reach are currently being enacted (e.g. Singapore and Malaysia), or revised (e.g. Australia and the EU), around the world (due in no small part to a desire to better address online privacy concerns) and their role is growing in importance, not least due to:

- the globalization of human interaction;
- the increasing commercial emphasis on data (many companies are built entirely on the data they hold);
- the increasing governmental interest in data access and processing;
- the increase in voluntary data sharing such as people posting, or otherwise distributing, their personal information on social networking sites;
- the 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;

- the increasing use of cloud computing where the geographical location of data may not be clear; and
- 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.

Furthermore, in seeking to predict the future relevance of data privacy law in the cross-border setting, it is interesting to contrast it to the field perhaps most closely related to it, namely defamation law. Internet defamation law has gained a considerable amount of attention. However, comparatively 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 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.

In essence, the conundrum we are faced with when dealing with the extraterritoriality of data privacy laws can be expressed as follows:

Extraterritorial jurisdictional claims are reasonable because if states do not extend their data protection to the conduct of foreign parties, they are not providing effective protection for their citizens. That is; protection must be afforded whatever the geographical source of the attack. In fact, it is possible to read *The International Covenant on Civil and Political Rights* (1966) as requiring states to make extraterritorial claims in the pursuit of protecting the privacy rights of the people within their jurisdiction.²

* Editor-in-Chief

** Editor

*** Managing Editor

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>> accessed 23 April 2013.

2 Dan Svantesson, ‘Fundamental policy considerations for the regulation of Internet cross-border privacy issues’ (2011) 3/3 *Policy & Internet*.

At the same time, extraterritorial jurisdictional claims are unreasonable because it is not possible for those active on the Internet to adjust their conduct to all the laws of all the countries in the world with which they come into contact. In other words, a widespread extraterritorial application of state law may well end up making it impossible for businesses to engage in cross-border trade.

To this can be added the international relations issues that may arise from too broad extraterritorial claims; that is, the broader extraterritorial claims one country makes, the more likely it is that it will intrude on the sovereignty of other states causing international friction. This issue should not be underestimated and as noted in the Australian Department of the Prime Minister and Cabinet's public discussion paper *Connecting with Confidence: Optimising Australia's Digital Future*:

Perhaps the greatest threat to an open, trusted, safe and secure digital environment is competition and conflict in

cyberspace between nations. To avoid this, understandings among states governing responsible online behaviour may need to be developed.³

Or to be more dramatic, we may recall that renowned international jurist Hugo Grotius noted that: 'where judicial settlement fails, war begins'.⁴ While it is unthinkable that war would spring from the effect the extraterritoriality of data privacy laws have on foreign business, it is prudent to remember that all matters of extraterritorial jurisdictional claims have consequences for international relations. Hopefully states and international organizations will finally come to realize the risks posed by the present uncertainty, and will embark on work to clarify jurisdictional rules as they relate to data privacy law.

doi:10.1093/idpl/ipt009

Advance Access Publication 19 May 2013

3 Department of the Prime Minister and Cabinet, *Connecting with Confidence: Optimising Australia's Digital Future* (18 October 2011), at 22 <http://www.egov.vic.gov.au/pdfs/connecting_with_confidence_public_discussion_paper.pdf> accessed 1 May 2013.

4 Stephen C. Neff (ed.), *Hugo Grotius On the Law of War and Peace* (Cambridge University Press, Cambridge 2012), at 81.