

Maurer School of Law: Indiana University Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship

2011

Editorial

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: <http://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., "Editorial" (2011). *Articles by Maurer Faculty*. 2613.

<http://www.repository.law.indiana.edu/facpub/2613>

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 wattn@indiana.edu.

Editorial

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

It is more than a decade since Scott McNealy, then CEO of Sun Microsystems, (in)famously declared: 'You have zero privacy anyway. Get over it!'¹ His statement caused quite a stir, and has since been quoted many times in various forms by both privacy sceptics and champions.

It turns out that rumours of the death of privacy were greatly exaggerated. Indeed, we are convinced that data protection and privacy law have never been more relevant or important than they are today. The fundamental principles of international privacy law set out three decades ago in instruments such as the OECD Guidelines and the Council of Europe Convention 108 have, on the whole, stood the test of time. Concepts such as fairness, transparency, lawful justification for processing, reasonable access to information, and appropriate security arrangements not only remain fundamental to regulation in this field, but are also are of growing interest and concern to individuals, businesses, and governments (see below).

However, it is fair to say that the practical application of these basic concepts has become increasingly strained. The following four key sources of stress also seem to be the main drivers behind recent calls for greater protection of privacy:

- The rapid, and relentless, development of technologies has had an extraordinary impact on data protection and privacy rights. While George Orwell was prescient in predicting some of the ways in which states would use surveillance technologies, even he could not anticipate the pervasive impacts of data processing and communications activities in both the public and private sectors. Today there is massive, and rapidly expanding, connectivity, with over a quarter of the world's population online and about half already using mobile phones. With Facebook alone boasting more than half a billion users, social networking services appear to have come of age. Meanwhile, concepts such as 'ubiquitous com-

puting' no longer seem fanciful, and the 'Internet of Things' is raising concerns about the practical consequences of massively distributed sensor networks and the applicability of privacy principles to data communications between devices as well as people. The proliferation of digital data and systems is also challenging the capacity of data protection and privacy regulation.

- A second key catalyst for revisiting the fundamentals of international privacy law is the globalization of the economy that, in one way or another, depends on cross-border transfers of personal data. International e-commerce is now well established and frequently gives rise to complex compliance issues for both providers and regulators of online transactions. More recently, outsourcing has developed from its early forms that were characterized by highly customized and heavily negotiated arrangements using stable and identifiable infrastructures, into a range of services based on fungible resources that are available on demand. Underlying this latter transition has been the emergence of cloud computing infrastructure, platforms, and services.
- Third, governments have demonstrated an apparently insatiable appetite for collecting data about individuals. Governments today increasingly rely on personal data to run social service programmes, administer tax programmes and collect revenue, support hundreds of regulatory regimes, maintain vital records about major lifecycle events, operate facilities, and enforce laws. The role of personal information collected as part of these programmes is striking, and reflects what Professor Paul Schwartz has described as the '*data processing model* of administrative control'. Professor Schwartz writes: 'Compared to its historic role, the state today depends upon the availability of vast quantities of information, and much of the data it now collects relates to identifiable individuals.'² Nowhere is this

* Editor-in-Chief

** Editor

*** Managing Editor

1 *Wired Magazine*, 26 January 1999.

2 Paul Schwartz, 'Data Processing and Government Administration: The Failure of the American Legal Response to the Computer' (1992) 43 *Hastings Law Journal* 1321, 1325, 1332 (emphasis in original).

clearer than in the push for greater security following the 9/11, London transport, and Madrid terrorist attacks. Governments now generate and collect an extraordinary volume of sensitive personal data in the name of national security, and increasingly rely on the private sector as the source of those data. Security agencies often evince little concern with privacy or data protection, courts are often tolerant of such behaviour, and even the public has shown itself willing to compromise privacy in the name of security. There is growing reason to fear, in the words of former UK Information Commissioner Richard Thomas, that we are 'sleep-walking into a surveillance society'.³

- Finally, despite many efforts at multinational cooperation over privacy protection, we have witnessed significant differences in the extent to which different national legal systems protect privacy, the tools used, and even the cultural norms about what constitutes 'privacy'. There is a growing realization about the need for greater harmonization of the various legal regimes for data protection and privacy, while realism compels the conclusion that any such harmonization will be a lengthy process that is fraught with obstacles.

These four factors suggest that data protection and privacy remains not only a vital subject, but also one requiring new and imaginative thinking. Until now there has been no scholarly journal with a truly global (rather than a national or regional) focus that is exclusively devoted to data privacy law. Moreover, in this area there is often a sharp divide between so-called 'academic' articles, which often lack sufficient connection to experience in the real world, and 'practical' ones, which many times fail to set forth a theoretical framework for considering the issues (which can be very useful to the practitioner as well). In the area of data privacy law, the distinction between 'scholarly' journals and 'practitioner' publications is often artificial and serves the interest of neither group. We will try to serve both communities, and will strive for our issues to be both intellectually stimulating and practically useful.

International Data Privacy Law (IDPL) has three main missions: to be global; to span the gulf between scholarship and practice; and to help solidify the position of data privacy law as a central area of importance for the individual, the economy, and the development of new technologies. We will be guided by the following main principles:

- IDPL will be truly global, in that it will not focus on a particular country, region, or legal system, and will cover developments around the world.
- We will focus on the area of 'data privacy' (eg, 'data protection' in the sense of the European Data Protection Directive 95/46, or 'information privacy' in the sense of the APEC Privacy Framework). We will generally not cover a number of other legal issues that may fall under the rubric of 'privacy' in certain legal systems, but that are only peripherally related to data or information privacy (eg, avoidance of being placed in a false light, protection of honour and reputation, reproductive rights, etc.).
- While we have a legal focus, we also welcome contributions dealing with economic, technological, and sociological issues, as long as they are related to the law in some way.
- We will publish articles of a high scholarly standard, but will always keep in mind the needs of practitioners.
- Since data protection and privacy law is such a fast-moving field, we will keep our eye not only on what the law is now, but on what it is likely to become.

We promise to do our best to be relevant, useful, international, thought-provoking, and to prove that data protection and privacy law are not only ready to enter the mainstream in the academic, business, and public sector worlds, but are in fact inescapable as well. We welcome your participation as readers, subscribers, contributors, and reviewers, and your input as to how we are doing and what we could be doing better.

doi:10.1093/idpl/ipq001

Advance Access Publication 5 October 2010

³ BBC News, 2 November 2006, available at: <news.bbc.co.uk/2/hi/uk_news/6108496.stm> (accessed 20 August 2010).