inter media
www.iicom.org
February 2013 Volume 41 Issue 1

by Chris Boam

Privacy in transition: The US and EU strive for meaningful change in the emerging 'economics of trust'

In the fall of 2002, I was involved in a lengthy meeting among industry attorneys debating whether a highly publicized (for the time) data breach the day before would or should change standard privacy compliance practices or depth of focus. The answers - many and varied - proved less memorable than one colleague's comment: "The American public's concern for privacy bad news is blissfully short." I remember that, not so much for the fact that what was said was - at the time - true, but because some of us around the table were sensing a rapidly approaching time when you could not say that and still keep your job. This was long before a public outcry would change the course of data usage for *Instagram*, or for that matter, when the changes to the privacy policies of Google or *Facebook* would be eagerly awaited by the user public and blogosphere like the prospect of a new Harry Potter movie. Almost as remarkable a moment for me came nearly a year later, in Brussels, when I had a meeting with an EU official. After I'd heard an extremely prolix description of how he viewed a provision of the data protection directive should be interpreted, I said, "It may be impossible to comply with that." His response - "Does it matter?"

Of course, neither of these colleagues had been engaged to view the US Federal Trade Commission's (FTC) struggle with the first iteration of the Children's Online Privacy Protection Act (COPPA). Likewise, neither had participated in the long protracted march from passage of the EU Directive 95/46/EC through vast piles of definitional interpretations and dense compliance recommendations to practices, procedures and costs that - though never truly comfortable - would only occasionally cause an executive to scowl or emit steam from the ears. Even so, the best and brightest might not have anticipated 2012. In one year, we saw the US introduce a cross-sectoral Consumer Privacy Bill of Rights (CPBoR) and a European Commission proposal seeking - among many other things - both data protection harmonization and dynamic views of what is "consent." How far have we come?

One of the most forceful articulations of privacy in US law is the 1967 decision of the Supreme Court in Katz v. US.[1] John Marshall Harlan II's concurring opinion established the "reasonable expectation of privacy" test, which contains a subjective component (actual expectation of privacy) and an objective component (reasonable expectation of privacy). However, it was the objective element that has had the unfortunate distinction of evolving into what has become known as the "third party doctrine" in the US - by which one diminishes or even loses an expectation of privacy through voluntary turnover of data to a third party (the quality of "voluntarism" is often a key factor in the application of this doctrine). The Obama Administration's 2012 CPBoR and accompanying white paper were introduced amid extensive deliberations by both the Federal Trade Commission (FTC) and Department of Commerce's National Telecommunications and Information Administration (NTIA).[2] Rather than a specific set of rules, the CPBoR is an affirmative statement of values - key among them are affirmation of the well-known Fair Information Privacy Principles (FIPPs)[3] and statements on the criticality of transparency (fundamental to what is "voluntary" under the Katz line of cases), access and user control. In addition to moving the ball quickly through work with industry on web-based do-not-track technology, the Administration has also engaged the NTIA to begin the multi-stakeholder process to better define key issue areas of data collection and use and applicable practices.

[1] http://supreme.justia.com/cases/federal/us/389/347/case.html

[2] http://www.ftc.gov/opa/2012/03privacyframework.shtm and http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf, http://www.ntia.doc.gov/page/privacy-report-introduction, respectively.

[3] e.g., http://www.ftc.gov/reports/privacy3/fairinfo.shtm

The Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPRs) system, although begun and developed through the Bush Administration, though US participation was only announced in July 2012. Acting US Commerce Secretary Rebecca Blank signaled the CBPRs as a key element to facilitate critical cross-border data flows in setting forth a common baseline of voluntary data privacy practices[4] for companies doing business among the 21 member countries of APEC and their 2.7 billion consumers. Many critical (and contentious) details remain to be debated in the US, including the scope of what constitutes "personal information," what equates to "consent" and in what way is it expressed, and what dynamic means of user control can and should be enabled. Remember, the CPBoR in the US, if embodied in law, is expected only to supplement existing statutes such as Gramm-Leach-Bliley Act on financial data, the Health Information Privacy Protection Act (HIPPA), and the Children's Online Privacy Protection Act (COPPA), among others. One need only review the commentary from the NTIA's most recent multi-stakeholder meeting (largely on mobile do-not-track issues)[5] or comments on the FTC's proposed revision of COPPA (e.g., covering sites "directed" (not targeted) to children)[6] to get a glimpse of the battle lines.

And of course, none of this touches upon what Congress may do in 2013, or for that matter, whether whatever the US may do will overcome foreign criticisms (particularly from the EU) over the voluntary nature of current proposals, the lack of a central enforcement agency for privacy, and other inhibitions to the US being recognized as an "adequate" environment for cross-border data transfers.

European Commissioner for Justice,Viviane Reding, announced sweeping proposals to change the Data Protection Directive 95/46EC in January 2012 in the form of a draft regulation. Among the many shakeups for data protection law in the proposal is the creation of a single supervisory authority (for companies in multiple EU jurisdictions), a broader concept of "personal data" and a slate of new definitions (e.g., "biometric data," "main establishment," and "personal data breach"), extra-territorial coverage, the "right to be forgotten," and substantial proceeds-based sanctions.[7] EU-based and multinational industry have praised the notion of replacing the directive with a regulation, which as a self-implementing instrument should greatly improve on harmonization among the 27 EU Member States over the decade-long game of 'over-and-under' that has been the national progeny of Directive 95/46/EC. Industry has been swift to recommend further improvements, for instance, to clarify what it means to have a "main establishment" and how this will impact your "supervisory authority," the inclusion of "privacy by design" and "privacy by default" concepts under the proposed rules, and how the new regulation would interplay with amendments to the Electronic Communications Data Protection Directive 2002/58/EC concluded as part of the Telecom Framework revisions of 2009.[8]

Thankfully, the notion of a "right to be forgotten" (RTBF, the proposed ability to wipe clean your net-based existence) seems to be dying of its own weight. However, even the conclusion by the European Network and Security Agency (ENISA) in November 2012, that the RTBF is "impossible," was embedded with problematic alternatives.[9] ENISA's proposed half-solution is to have search engines 'blacklist' data that a user would not want to be found. Imagine what such a tool could be used for in morally questionable hands, or for that matter, the mess it would make of the right to free expression under Article 10 of the European Convention on Human Rights.[10] On data breach notification, European Commissioner for the Digital Agenda Neelie Kroes is forging ahead with a proposal to both introduce and harmonize an EU-wide set of requirements - also an aim of the proposed regulation - to supplant the existing patchwork of mandatory (e.g., Germany) and voluntary (e.g., UK) national rules. With the right balance clearly struck, to harmonize procedures and deadlines only when notification would be necessary and useful to consumers, the requirements could potentially alleviate the costs of current single market confusion on the issue.

[4]http://www.hldataprotection.com/uploads/file/White%20Paper.pdf

[5]http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

[6]http://www.ftc.gov/opa/2012/08/coppa.shtm

[7]http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[8]e.g., http://www.ectaportal.com/en/PRESS/ECTA-Press-Releases/2011/Industry-Joint-Statement-on-EU-privacy-framework/-print/

[9]http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten

[10]http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf

Industry engagement on these issues in Brussels has been among the most focused and consistent I've seen in a number of years. Emblematic is the input of the International Chamber of Commerce (ICC),[11] which seeks improvements to the draft regulation to facilitate clear but limited obligations combined with flexible compliance options (e.g., greater flexibility for the use of binding corporate rules (BCRs) and model contract clauses). Many in Europe understand the stakes and concur that a desire to overhaul data protection is in no small measure a goal to both further enable net-facilitated economic growth (through clarity) and not inhibit technical innovation (through a continued density of EU rules). Unlike my colleagues of 8-10 years ago, many today not only "get it," but also, are working feverishly to achieve change. Whether you agree with, for instance, Lord McNally's September 2012 testimony before the UK Parliamentary Select Committee on Justice that the proposed regulation could or should be converted into a directive,[12] or German Member of the European Parliament Alexander Alvaro's proposal for rules outlining "lifecycle data protection management,"[13] you cannot deny that these and many others are fully and thoughtfully engaged.

[11]http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2013/ICC-comments-EU-Gen-DP-Reg-Issues/

[12]http://www.parliamentlive.tv/Main/Player.aspx?meetingId=11425

[13]http://www.alexander-alvaro.de/inhalte/lifecycle-data-protection-management-a-contribution-on-how-to-adjust-european-data-protection-to-the-needs-of-the-21st-century/

They have to be. As the New York Times reported on January 16, 2013, 4 in 10 EU consumers avoid making online purchases because concern about the security of their personal data.[14] In truth, I believe that the 4 in 10 are less concerned with whether it is indeed secure than with how do they know that it is and who to and under what authority do they seek to address a problem. As MEP Alvaro observed, the Commission proposal does not "solve the problem that many consumers are simply overwhelmed by the amount of information they are provided with." Similarly in the US, Brookings Fellow Allan Friedman observed, consumers need statements that are "easier to understand, and control easier to enact."[15] Transparency needs to be concise, meaningful and useful. And, while the need for a clear 'check box' of consent is - for lawyers - a holy grail on both Atlantic coasts, the consumers (and their choices) far too often fall down the rabbit hole of interminable language as they pull the lever labeled, "I agree." This, in part, treads upon the notion of what is or is not truly "voluntary" in the Katz line of case law in the US.

Despite how much has changed since 2002-03, and all the attention paid to each and every edit to industry privacy practices, some consumers still do not care, and that's fine, since it is to be expected. However, a growing number vocally do care. Gone are the days when "shame based regulation" - a firm would overstep some boundary and get momentarily pilloried in the press - can represent the worst of expectations.

[14]http://www.nytimes.com/2013/01/17/technology/17iht-data17 html?pagewanted=all&_r=0.

[15]http://www.brookings.edu/blogs/up-front/posts/2012/02/29-internet-privacy-chat.

US and European consumers still stand to know more about what their browser and computer is daily telling the world, and take advantage of browsers, plug-ins and other practices that minimize data sharing. In the midst of legislative shifts on privacy as significant as those signaled in 2012, as Allan Friedman of Brookings puts it, "competition based upon the 'price' of less intrusive data collection" is moving ever closer to an elemental part of good business. As Marc Rotenberg, head of the Electronic Privacy Information Center, said in September 2012, "how do you consent to the disclosure of your information if you don't know which of your information will be disclosed, to whom or for what purpose?"[16] In such an environment, where such questions continue to linger and are debated in the blogosphere, finding ways to engage customers in the dialogue, while respecting their privacy and giving them control over their own data, may ultimately create far more opportunities for innovation. In the absence of this engagement, the 'economics of trust' - the moment when a lack of comfort, either in transparency or follow-through translates to a consumer's decision not to press "send," "purchase," or "I agree" may become an ever more measurable reality.

Chris Boam is Principal in the US-based consulting firm 40A&M LLC http://www.40a-m.com/

[16]http://news.cnet.com/8301-13578_3-57516501-38/senators-prepare-to-vote-on-netflix-and-e-mail-privacy/.