Privacy in Transition: the U.S. and EU Strive for Meaningful Change in the Midst of Emerging 'Economics of Trust'

Christopher Boam [1]

In the fall of 2002, I was involved in a lengthy meeting among a select few 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 on the day than one colleague's comment. "The American public's concern for privacy bad news is blissfully short." I remember that moment vividly, 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 day rapidly approaching when you could not say that and (as my British friends say) still keep your station. Bear in mind, this was long before a public outcry would change the course of data usage for Instagram, or for that matter, where the changes to the privacy policies of a Google or Facebook would be eagerly awaited by the user public and blogosphere like the prospect of a new Harry Potter installment. 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 U.S. 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's '95 directive 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 a year, we saw the U.S. introduce a cross-sectoral Consumer Privacy Bill of Rights (CPBoR) and white paper 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 U.S. law is the 1967 decision of the Supreme Court in Katz v. U.S.[2] John Marshall Harlan'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 U.S. – by which one diminishes or even loses an expectation of privacy through voluntary turnover of data to a third party (the quality of "voluntarism" often a key factor in the 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 National Telecommunications and Information Administration (NTIA).[3] 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) [4] 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 spearhead the multi-stakeholder process to define key issue areas of data collection and use and applicable practices.

The Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPRs) system, although begun and developed through the Bush Administration, was finally brought to announced U.S. participation in July 2012. Acting U.S. 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[5] for companies doing business among the 21 member countries of APEC and their 2.7 billion consumers. But while the CBPRs may serve as a long sought-after set of cross-border top line rules, within the U.S., many critical (and contentious) details remain to be debated, 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 U.S., if embodied in law, is expected only to supplement existing statutes such as Graham-Leach-Bliley (GLB, 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) [6] or comments over the past year on the FTC's COPPA proposed rule and additional revisions[7] to get a glimpse of some of the continuing battle lines. And of course, none of this touches upon what Congress may do in 2013, or for that matter, whether what anything the U.S. 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 U.S. being recognized as an "adequate" environment for cross-border data transfers.

EU Commissioner Viviane Reding announced sweeping changes to the Data Protection Directive of 1995 in January 2012 in the form of a draft regulation. Among the many shakeups for data protection law in the proposal include creation of a single supervisory authority (for companies in multiple EU jurisdictions), a broader concept of "personal data" and 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.[8] 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 the '95 Directive. Industry has also been swift to recommend needed 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 proposed rules, and how the new regulation would interplay with amendments to the 2002 Directive (the Electronic Communications Data Protection Directive) concluded as part of the Telecom Framework revisions of 2009.[9]

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," itself was embedded with problematic alternatives.[10] 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 could make of the right to free expression under Article 10 of the European Convention on Human Rights.[11] And 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., German) and voluntary (e.g, U.K.) national rules.[12] 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.

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),[13] which seeks improvements to the draft regulation to facilitate clear but limited obligations combined with flexible compliance options (e.g., greater flexibility for use of binding corporate rules (BCRs) and model contract clauses, etc.). 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 above of 8-10 years ago, many today not only "get it," but also, are working feverishly to achieve change. And whether you agree with, for instance, Lord Thomas McNally's September 2012 testimony before the U.K. Parliamentary Select Committee on Justice that the proposed regulation could or should be rolled back to a directive,[14] or German Member of the European Parliament Alexander Alvaro's proposal for rules outlining "lifecycle data protection management,"[15] you cannot deny that these and many others are fully and thoughtfully engaged.

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.[16] In truth, I believe that the 4 in 10 are likely 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."[17] Similarly in the U.S., Brookings Fellow Allan Friedman observed, consumers need statements that are "easier to understand, and control easier to enact." [18] 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 saying, "I agree." This, in part, treads upon the notion of what is or isn't truly "voluntary" in the Katz line of case law in the U.S.

Why then, if we do indeed have many of the same aims, do we still seem not only to be oceans apart, but also, far collectively from these goals? The first obstacle is both historic and structural. In June 2011, Omer Tene wrote a brief but wonderful piece for the Center for Democracy and Technology (CDT) in which he characterized U.S. versus European schools of thought regarding privacy law.[19] In short, he states that the density of EU law is emblematic of the thinking that enshrines privacy fundamentally as respect for the individual, a respect that is established and protected by a Hobbesian density of rules. By contrast, the U.S. view of privacy is one where a citizen simply asks to be "left alone" and law helps define where and when this might be a reasonable notion. For non-lawyers, consider the analogy in schools of acting. Europe's privacy character is method – built from within and rooted in the history of government intrusiveness run amok in World War II (e.g., Strasberg), whereas the U.S. character is built from the external with trappings of makeup and costume (e.g., Olivier). For lovers of early 1980s electronica music, it's the warm blanket of sound from subtractive synthesis (e.g., Korg Poly 800 engineering) versus the harsh tones of additive synthesis (e.g., Yamaha DX7 engineering). You get the point. In this environment, the continued seeking of mutual recognition best practices among the EU and U.S. privacy frameworks by the Obama administration and EU is a difficult goal, but I give them great credit for continuing to try.

Second, the complexity and continuing advancement of communications technologies and applications, and the potential impacts of data collection and usage (or *ex ante* limitations) requires a deliberate careful march. It is no accident – though surely frustrating for business – that the European approaches to privacy rules for the Internet of things[20] and/or applicability to cloud services[21] will both impact and be impacted by the long process associated with vetting of the proposed regulation. This is also why comment processes, like the one discussed above at the FTC for COPPA, are critical. For instance, one of

the lingering criticisms after the revision went final in December 2012 is the seeming expansion on the notion of "directed to" to include "targeted to" under the scope of what is a covered site and when that status might trigger the need for age vetting.[22] If the scope of coverage is at all vague, the impact could be for some businesses to err on the side of caution – more age verification – and what may be unnecessary collection of more personal data. In the EU, if filtering or traffic redirecting tools are mandated – as suggested above by ENISA – the lists of possible uses and impacts to networks would be endless. This is similar to the dangers that U.S. lawmakers quickly became cognizant of in the debate of legislation like the Stop Online Piracy Act (SOPA) in 2012. It is also in part for this reason that legislators like Dutch Member of the European Parliament Marietje Schaake, in her August draft report on digital strategy, urged EU institutions to include conditionality clauses in negotiated agreements with third countries stipulating the need to respect and preserve unrestricted access to the Internet, digital freedoms and human rights online.[23] Similar emphases have been a cornerstone of U.S. Department of State engagement on digital rights for some time.[24]

Third, both camps remain hobbled to a degree by inconsistency, intransparency and an at-times inelegant way that they have dealt with the privacy issues attendant to the cyber and physical security realities of today's world. In March 2012, the European Data Protection Supervisor – whose non-binding opinions are nonetheless among the most authoritative under EU law – expressed dismay that the proposed regulation relegated data protection for law enforcement to a thin separate legal instrument of inferior quality to the draft regulation.[25] In addition, since April, much has been made of U.K. announced plans for a nationwide electronic surveillance network, centralized database of certain email and phone traffic, and closed door non-judicial assessment of when intelligence gathering is in the "national security interest."

To a certain extent, these issues resulted initially in EU-U.S. 'chest thumping' with at-times diametrically opposed explanations – e.g., "our laws and law enforcement authorities do pretty much the same things in the same way," and on privacy generally, "our fundamentals are better than theirs." Most law enforcement and intelligence gathering efforts are understandably not the domain of publicists. However, explanations and the pace of events have not been a friend to either side on these issues. Theoretically, for instance, investigative access to retained data in the U.K. should not be about the content, but some Home Office statements actually muddied the water, saying "it's about the who, what, where and when."[26] That sounds like content to me, whether it is or not.

The threats are certainly real. And, in the U.S., the wave of cyber-security cover stories this fall in the Washington Post stand testament to the desire to have the public understand that reality.[27] When the Cyber Intelligence Information Sharing Protection Act (CISPA)[28] failed to pass the Congress in the fall of 2012, the Administration began a concerted effort to develop a stop-gap though limited Executive Order to enable voluntary information sharing among service providers and with government entities of data deemed of a "cyber-security purpose" or for the "protection of the national security of the U.S." By any measure, the Administration's outreach in developing an executive order – to industry, civil society, law enforcement – has been unprecedented, and if reports are correct, it may be in place by the time you see this article.[29] But, many questions in the U.S. will be left unanswered. What is a "cyber incident" or a "threat," what incentive is there to limit information intercepted or disseminated, and will there be oversight audits?[30] Even serious reform of the Electronic Communications Privacy Act (ECPA), which would have mandated a court order for opening the content of an email, fell from the legislative horse that it had for so long ridden – the Video Privacy Protection Act – moments before it was sent to the President for signature in the week before Christmas.[31] Similar to the intent of the CISPA, the ECPA contains an exception for a service provider to access – though not share – email and other communications content to "protect its network," but case law has limited this exception to narrowly tailored action by the service provider

with a substantial nexus to the concern. The courts have left little room for frolic and detour.[32]

This is not to say that I am in any way suspicious of our communications service providers and their seriousness with regard to obligations to both customer and government. I have worked with these colleagues for many years, and many of these folks I regard as committed not only to the critical role they play in national security, but also, to the consumer rights issues for which they may often stand as the last best defense – true patriots in the finest, most limited sense of the word. But, I'm reminded of Plato's parable of the Ring of Gyges and Plato's brother Glaucon.[33] Glaucon believed that, when you are vested with the power to move through life and data invisibly, even the just man will succumb to his appetites. I am not a Glauconist. Like Socrates, I believe that the just man (or woman) can continue to be just even with extraordinary power. With cyber-security, information sharing, and the possible free expression restraints that can be exercised through access to content, however, I must leave open the possibility that Glaucon may be right.

To this end, the Privacy and Civil Liberties Oversight Board (PCLB)[34] on October 23, 2012 announced its first meeting. At that meeting, suggestions for the PCLB's attention were voluminous, including information sharing, the Patriot Act and use of its section 215, FISA, DHS fusion centers and secret Office of Legal Counsel memos, among others.[35] On December 15, President Obama nominated two more members to the PCLB and David Medine, long known and respected for his work on issues of privacy internationally, as its Chairman. The hope is that the PCLB can cull this list to a few near-term actionables, and when the time comes, the Department of Justice will step up if needed to respect a request from it for investigative action enabling its work.

How or if these developments could impact the substance of CISPA-like legislation that may get introduced in the U.S. in 2013 remains to be seen. It has been underscored that the need for firms to voluntarily share security-critical information cannot be hobbled by broad and open liability visited upon participating firms. If there are to be liability limitations applied to a legislated voluntary sharing program, in addition to the efforts of the PCLB, perhaps an acceptable 'check' might be to have participants be 'sponsored' by their applicable regulator (e.g., FTC, FCC). Criticism for malfeasance in information sharing could be visited upon the sponsor, perhaps resulting in immediate sunset of the program. Loss of credibility before a regulator would be, of course, its own penalty, but it would not have the immediacy of liability and related costs.

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. It's 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. Sure, U.S. and European Consumers can 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. But in the midst of privacy shifts 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?"[36] In such an environment, where such questions continue to linger and are debated in the blogosphere, finding ways to engage users in the dialogue, while respecting their privacy and giving them control over their own data, may ultimately create far more opportunities for innovation.[37] In the absence of this engagement, the 'economics of trust' – the moment when a lack of comfort, either in transparency or follow-through by industry or government translates to a consumer's decision not to press "send," "purchase," or "I agree" – may become an ever more measurable reality.

End Notes

[1] Chris Boam is Principal in the U.S-based consulting firm 40A&M LLC (http://www.40a-m.com/who-we-are.html).

[2] *See* 389 U.S. 347 (1967), *available at*: supreme.justia.com/cases/federal/us/389/347/case.html.

[3] *See*, *e.g.*, Protecting Consumer Privacy in an Era of Rapid Change, Federal Trade Commission Report (March 2012), available at: www.ftc.gov/opa/2012/03/privacyframework.shtm; Internet Policy Task Force Privacy Green Paper, U.S. Dept. of Commerce, NTIA (Dec. 2010), available at: www.commerce.gov/node/12471; Internet Policy Task Force-Privacy (update pages, including multistakeholder process), U.S. Dept. of Commerce, NTIA (last visited Jan. 2013), *available at*: www.ntia.doc.gov/category/privacy.

[4] *E.g.*, Fair Information Privacy Principles, Federal Trade Commission, *available at*: www.ftc.gov/reports/privacy3/fairinfo.shtm.

[5] *See*, *e.g.*, APEC Cross-border Privacy Rules System Program Requirements (for use in conjunction with the APEC CPBR Intake Document), *available at*: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-ProgramRequirements.ashx.

[6] *See*, *e.g.*, U.S. Dept. of Commerce, NTIA, Privacy Multistakeholder Process (mobile app. transparency), *available at*: www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[7] *See* Children's Online Privacy Protection Act, Comments on Federal Trade Commission Proposed Rule, available at: www.ftc.gov/os/comments/copparulereview2011/; *e.g.*, CDT and ALA Supplemental NPRM Comments (in FTC Project No. P104503), *available at*: https://www.cdt.org/files/pdfs/CDT-ALA_Supplemental_NPRM_comments.pdf.

[8] *See* Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, Eur. Comm., COM(2012) 11 final (Brussels, 25 Jan. 2012), *available at*: ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; European Commission (update pages, last visited Jan. 2013), *available at*: ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[9] *E.g.*, EABC EU Data Protection Regulation: Analysis and Prescriptions for Reform (June 22, 2012), available at: static.squarespace.com/static/50a3f5e4e4b072e097b3426f/t/50d1f5c5e4b026536deca9de/1355937221046/EABC%20EU%20Data%20Protection%20Regulation%20Side-by-Side%20Analysis%20-%202012%20June%2022.pdf.

[10] *See* The Right to be Forgotten – between Expectations and Practice, European Network and Information Security Agency (ENISA) (Nov. 20, 2012), *available at*: www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten.

[11] European Convention on Human Rights, *available at*: www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf.

[12] *See*, *e.g.*, Kevin O'Brien, Europe Weighs Requiring Firms to Disclose Data Breaches, New York Times (Jan. 16, 2013), *available at*: www.nytimes.com/2013/01/17/technology/17iht-data17.html?pagewanted=all&_r=0.

[13] *See* ICC Comments on EU General Data Protection Regulation Issues (Jan. 21, 2013), *available at*: www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2013/ICC-comments-EU-Gen-DP-Reg-Issues/.

[14] *See* Hearing on EU Data Protection Framework Proposals, UK Parliament, HOC Justice Committee (Sept. 17, 2012), *video of hearing available at*: parliamentlive.tv/Main/Player.aspx?meetingId=11425.

[15] *See* Alexander Alvaro, Member of the European Parliament (Germany), Lifecycle Data Protection Management – a Contribution on how to Adjust European Data Protection to the Needs of the 21st Century (Oct. 3, 2012), *available at*: 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/.

[16] *See*, *e.g.*, O'Brien, *supra* note 12.

[17] Alvaro, *supra* note 15, at 4.

[18] Allan Friedman, Web Chat: Protecting Online Privacy, Brookings: Up Front (Feb. 29, 2012), *available at*: www.brookings.edu/blogs/up-front/posts/2012/02/29-internet-privacy-chat.

[19] Omer Tene, Privacy in Europe and the U.S.: I know it when I See it, Center for Democracy and Technology (June 27, 2011), available at: www.cdt.org/blogs/privacy-europe-and-united-states-i-know-it-when-i-see-it.

[20] *See*, *e.g.*, Digital Agenda: Commission Consults on Rules for Wirelessly Connected Devices – the 'Internet of Things', European Commission Release and Consultation (April 12, 2012), *available at*: ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=8002.

[21] *See*, *e.g.*, Article 29 Working Party Opinion 05/2012 on Cloud Computing, European Commission (July 1, 2012, *available at*: ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf; Digital Agenda: New Strategy to Drive European Business and Government Productivity via Cloud Computing, European Commission Release IP/12/1025 (Sept. 27, 2012), *available at*: europa.eu/rapid/press-release_IP-12-1025_en.htm?locale=en.

[22] *See* Children's Online Privacy Protection Rule, Federal Trade Commission (Dec. 19, 2012), *available at*: ftc.gov/os/2012/12/121219copparulefrn.pdf (see

paragraph (c) of the final rule and the FTC's commentary on it, pages 48-52).

[23] *See* European Parliament Endorses First Ever Digital Freedom Strategy, Release of Marietje Schaake, Member of the European Parliament (Netherlands) (Dec. 11, 2012), *available at*: www.marietjeschaake.eu/2012/12/european-parliament-endorses-first-ever-digital-freedom-strategy/; European Parliament Draft Report on a Digital Freedom Strategy in EU Foreign Policy, Committee on Foreign Affairs (2012/2094(INI)) (Sept. 2012), at p11 ¶35, *available at*: www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bREPORT%2bA7-2012-0374%2b0%2bDOC%2bPDF%2bV0%2f%2fEN.

[24] *See*, *e.g.,* Michael H. Posner, Internet and Academic Freedom in the Digital Age, U.S. Dept. of State Official Blog (Oct. 18, 2012), *available at*: blogs.state.gov/index.php/site/entry/freedom_digital_age.

[25] *See* Opinion of the European Data Protection Supervisor on the Data Protection Reform Package (March 7, 2012), *available at*: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.

[26] *See*, *e.g.*, Raphael Satter, UK Internet Group Warns Goivernment is Mulling Plans for Mass Electronic Surveillance Program, Associated Press (April 1, 2012), *available at*: www.thestar.com/news/world/article/1154947--u-k-internet-group-warns-government-is-mulling-plans-for-mass-electronic-surveillance-program.

[27] *See*, *e.g.*, Zero Day – the Threat in Cyberspace, series of Washington Post special reports (last visited Jan. 2013), *available at*: http://www.washingtonpost.com/investigations/zero-day.

[28] Stop Online Piracy Act, H.R. 3261 (introduced Oct. 2011), *available at*: www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf.

[29] *See*, *e.g.,* Jennifer Martinez, Obama Likely to Issue Executive Order on Cybersecurity as Early as January (Dec. 21, 2012), *available at*: thehill.com/blogs/hillicon-valley/technology/274175-cybersecurity-order-likely-in-january-observers-say.

[30] *See*, *e.g.,* Comments of the Electronic Privacy Information Center, in Defense Industrial Base Voluntary Cyber-security and Information Assurance Activities (July 10, 2012), available at: epic.org/privacy/cybersecurity/EPIC-DOD-Cyber-Security-Comments.pdf.

[31] *See*, *e.g.*, Netflix Social Sharing Bill Passes without Email Privacy Protection, Huffington Post (Dec. 26, 2012), *available at*: www.huffingtonpost.com/2012/12/26/netflix-social-sharing-bill_n_2367385.html.

[32] *E.g.*, McClelland v. McGrath, 31 F.Supp.2d 616 (N.D. Ill. East. Div.) (Nov. 23, 1998), available at: www.leagle.com/xmlResult.aspx?xmldoc=199864731FSupp2d616_1574.xml&docbase=CSLWAR2-1986-2006.

[33] *See* Dialogues of Plato, 4th Tetralogy - 2nd Dialogue (last visited Jan. 2013), *available at*: plato-dialogues.org/tetra_4/republic/gyges.htm.

[34] *See*, *e.g.*, Garrett Hatch, Privacy and Civil Liberties Oversight Board: New Independent Agency Status, Congressional Research Service Report (Aug. 27, 2012), *available at*: www.fas.org/sgp/crs/misc/RL34385.pdf.

[35] *See* Rachel Levinson-Waldman, the Privacy and Civil Liberties Oversight Board: an Opportunity to Limit Data Retention and Sharing, Brennan Center for Justice (Nov. 9, 2012), *available at*: www.brennancenter.org/blog/archives/the_privacy_and_civil_liberties_oversight_board_an_opportunity_to_limit_dat/.

[36] Declan McCullagh, Senators Prepare to Vote on Netflix and Email Privacy, CNet (Sept. 20, 2012), *available at*: news.cnet.com/8301-13578_3-57516501-38/senators-prepare-to-vote-on-netflix-and-e-mail-privacy/.

[37] *Cf.*, Friedman, *supra* note 18 (also on the importance of engagement, respect and control).