U.S.-EU Privacy Policy Relations Post-Snowden: 'Keep Calm and Carry On' Over A Perilous Road

By Chris Boam, Founder and Principal of 40A&M LLC Consulting

On a foggy night in October 2003, my wife and I found ourselves late for an expected arrival in Tralee, County Kerry, Ireland. Shortly after dark, we entered a part of the Dingle Peninsula route known as the Conor Pass, not being at all adequately briefed as to what this road entailed. At one point, my wife – who had taken over the driving – asked me what I was looking at. The real answer was indeed "nothing," for despite the pitch-blackness, it had been clear to me for at least a mile that we were driving along the edge of a shear cliff face. I did my best at being nonchalant. "Just keep focused on the road ahead, and we can talk about it in Tralee." We did arrive safely, but still, I made sure that we ordered pints before looking at guidebook pictures of the Pass.

Like traversing the Conor Pass, the U.S.-EU privacy policy positioning looks perilous for practitioners and policy-makers alike, but the best course for both sets of parties may be to "keep calm and carry on." When I wrote in January that the EU-U.S. privacy relationship had several fundamental stumbling blocks despite many mutual goals, I did not expect that "investigative measures" would soon dominate the news. It's not that we didn't already have a fair amount of drama around significant privacy and related cyber-security developments heading into June. The European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) had already delayed its vote on a revised draft data protection regulation until May, and then again until June in the wake of over 3,000 tabled amendments. Consideration is now scheduled for October.

In the wake of the June revelations from Edward Snowden, reactions were swift and pointed, both in the U.S. and Europe. One of the first developments in Europe was the rumor that the so-called 'Article 42' to the draft regulation was being revived-- a provision that would force multinational companies to disclose to European data subjects that another country has (secretly) requested their data. In early July, Parliament voted to give its support to the Commission to end the Swift and other data-sharing programs with U.S. authorities, should the Commission choose to exercise that power. And in the final week of July, Vice President Viviane Reding announced that the Commission would conduct a "solid assessment" of the data protection Safe Harbor program with the U.S., engaging for the first time its Article 3 powers to possibly suspend the program if it deems that standards are not being met. Even MEPs who had heretofore been bullish to ensure that the draft regulation accomplish twin goals – ease impediments to international data flows and enshrine a set of truly single market rules – have been reduced to stressed understatement: "a balanced position on privacy is needed … but certainly the surveillance revelations have come as a blow," said Irish Conservative in the European Parliament, Sean Kelly, who has been in forefront of efforts to make EU privacy laws more business friendly.

The potential loss of these advocates could be devastating for industry, and particularly the U.S. tech industry. A June 21st segment hosted by National Public Radio's Tom Gjelten was one of the first post-Snowden discussions I'd heard regarding a potential foreign industry backlash to "avoid American cyberspace." By early August, the Information Technology & Innovation Foundation (ITIF) had published a brief outlining potential impacts to the U.S. cloud computing industry. Out of a global enterprise cloud computing market of $207 billion by 2016, ITIF suggests that, on the high-end, U.S. cloud providers could lose $35 billion. Some European legislators have jumped into this fray. Neelie Kroes, European Commissioner for Digital Affairs, opined: "if European cloud customers cannot trust the U.S. government, then maybe they won't trust U.S. cloud providers either." Still others are trying to take the pulse of consumer concerns, with one outlet reporting in mid-August that after seven weeks of post-Snowden media coverage, the percentage of Internet users reporting concerns about their privacy online jumped from 48 to 67 percent. Some business model impacts have been immediate, with both Texas-based Lavabit and Seattle-based Silent Circle shutting down their secure email services in part because they could no longer ensure their commitments to market these services as truly private. In a July 13 legal filing in the Northern District of California, Google seemed to be admitting similar with regard to its Gmail service, though unlike Lavabit and Silent Mail, Gmail had never been marketed as secure.

Just after the Guardian revealed XKeyScore on July 31st, the Obama administration took some significant steps toward both policy defense and public relations. This began with General Keith Alexander's unprecedented appearance before the 'Black Hat USA 2013' hackers conference in Las Vegas, Nevada on July 31st. This was followed on August 9th by release of a 23-page memorandum and cover note setting forth a legal defense for the NSA's surveillance measures, and in particular, use of the Patriot Act's Section 215 authority. Whether you agree with the broad strokes of the memorandum or not, the fact that we could read it at all was impressive. Concurrent with release of the memo, President Obama held a news conference to propose four changes to the NSA programs, including introduction of an adversarial component to FISA court hearings and greater oversight authority over measures taken under Section 215. The President also announced plans to establish a new task force to analyze the surveillance programs, although it's unclear how or if this will complement efforts already undertaken by the Privacy and Civil Liberties Oversight Board (PCLOB).

These efforts were set back on August 15th when the Washington Post released findings of an internal audit it had obtained,

detailing that the NSA had broken privacy rules applicable to the surveillance measures "thousands of times" through 2012, with some analysts even using the surveillance tools for personal ends. The released papers also included a stiff rebuke from the FISA court in October 2011 that found the NSA's methods "deficient on statutory and constitutional grounds." Although shocking and a critical milestone in the events of the past two months, the preceding week to ten days seemed to foreshadow what the audit papers ultimately revealed. For although the NSA had emphasized that "multiple technical, manual and supervisory checks and balances" were employed to prevent data misuse, and that access to NSA's analytic tools is "limited," the very person who brought these issues to light – Edward Snowden – had, according to Booz Allen, "been on our payroll for a short period of time" and "did not share our values." That's a striking dichotomy. Similarly, when the U.K. government insisted that the Guardian destroy a hard drive containing NSA-related background, and then used Schedule 7 authority under the Terrorism Act of 2000 to detain the partner of a Guardian journalist, this was hardly – in the parlance of public relations – getting in front of the story.

However, as early as the first week after the NSA revelations, anger and questions in Europe regarding the surveillance measures also began to be focused inward, asking of European and Member State authorities 'how much they knew' and 'when did they know it.' By mid-July, the Washington Post was reporting that American surveillance and allegations of German complicity, in particular, had become a campaign issue in that country. Also, early outrage regarding the NSA programs from government authorities in France was tempered on July 4th when Le Monde reported that France's foreign intelligence service, the DGSE, was engaging in surveillance similar to Prism on connections within France and between France and other countries. The news was somewhat reminiscent of Captain Renault's "shock" in Casablanca that gambling was going on at Rick's cafe, just as he turned to say "thank you" to an attendant for delivering his winnings. On June 20th, attorney Christopher Wolf wrote an excellent op-ed outlining Internet and phone call data surveillance measures that also occur in Europe. And whether you agree with comparative strength of this defense and its "they're doing the same" nature or not, it effectively checks any naiveté you might bring to its reading. As a result, however, European sentiment toward its own version of data protection has quickly become far more entrenched.

For these and myriad other reasons, U.S. and EU officials necessarily took action in the first week of July to carve-out data protection issues from consideration in trade negotiations toward a TransAtlantic Trade and Investment Partnership (TTIP). Talks regarding privacy were to take place separately but "in parallel," so as to not have key prospects for growth-through-trade weighed down by continuing surveillance revelations. However, U.S. and EU negotiators recognize that these discussions in the separate data protection working group will eventually be integral to TTIP negotiations on Internet and e-commerce issues. Although critical to the negotiating process, the carve-out hardly eliminates hard questions.

"What happens now," you might ask. Well, for starters, it is not surprising that we've heard little in recent months regarding the Cyber Intelligence Information Sharing Protection Act (CISPA), or for that matter, expansion of the Communications Assistance for Law Enforcement Act (CALEA). Both were front-and-center agenda items in the U.S. in April, and the fact that these and related initiatives have gone quiet is both unfortunate and necessary. Like it or not, the Snowden revelations have changed the landscape, irrespective of whether the relevance of privacy and investigative measures – as a topic – merits so broadly applicable a fallout that has sprung from the leaks.

Since the Obama Administration's August 9th release of its legal memoranda, debate has continued as to whether Members of Congress were (or today feel that they were) adequately briefed to endorse the surveillance measures as the memo emphasizes that they did. FISA Court Chief Judge Reggie Walton has also said that the court lacks the tools to "independently verify how often the government's surveillance breaks the court's rules." Even early Congressional defenders of the programs have found most recent admissions "deeply disturbing." The Privacy and Civil Liberties Oversight Board (PCLOB), meeting for 7 hours in its first public hearing on July 9th, intends to prepare a report with recommendations on the NSA programs. Some of these discussions may focus in on whether the third-party doctrine, long a tenet of U.S. privacy law, applies to today's Internet communications and meta-data just as neatly as citation of the 1978 Supreme Court opinion in Smith v. Maryland, which held that the collection of call records (who called whom and when) is not a 'search' within the meaning of the Fourth Amendment, might imply that it does.

Even as these necessarily deliberative processes begin, of course, nothing else will stop. Although few may have read about them, draft privacy legislation has been tabled in Brazil, and far-reaching measures have been passed in Texas and introduced (though delayed) in California. The potential impacts of these and other proposed measures on commerce, irrespective of protective motives, will need to be reviewed and considered. In addition, trialogue discussions, among EU Council, Parliament and Commission, are continuing, with the aim of ironing out disagreements and conflicts over amendments. The Civil Justice Liberty and Home Affairs (LIBE) Committee now plans to have a vote on the draft regulation in October. Key among the remaining issues in the text involve its territorial scope (Article 3), the nature and quality of consent and when it is given (Article 7), a slate of new definitions (e.g., "biometric data," "main establishment," and "personal data breach"), and the fate of the so-called "right to be forgotten." And even as these issues are debated in trialogue, a new EU data breach regulation, pursuant to Directive 2002/58/EC, came into force on August 24th with the aim of ensuring consistent requirements across the EU for businesses and data subjects.

On one end of the spectrum is the call for privacy issues to simply 'cede the floor,' in view of advancing technology, NSA revelations. Judge Richard Posner, pre-eminent U.S. jurist on the U.S. 7th Circuit Court of Appeals wrote an op-ed in the New York Daily News in April, calling privacy "overrated." Although the article's premise is sound – that issues of security and the public interest will at times outweigh privacy concerns in the balance – its strident tone might have been heard more tolerantly in a pre-Snowden world. An August 12th article in Time magazine posited, unconvincingly, that privacy is simply "illusory." Even Alex Karp, CEO of Palantir and one of the most successful developers of "big data" analytical tools agrees that, as a society, we must find "places that we protect," so that we can "all be unique and interesting." The notion that we should simply "throw up our hands" and admit that there will be no more private space – as if the 'third party' in the parlance of U.S. doctrine exists in the home and everywhere like some omniscient force – is simply too Orwellian for an ordered society.

But on the other end of the spectrum, I have to agree with attorney Eduardo Ustaran, whose June 12th op-ed was spot-on. It would be "unfair that a data collection and analysis program, which is entirely motivated by national security reasons, causes a raising of the bar for organizations which are completely outside the scope of the program." Despite the unfairness, this may be the current lay of the land. In the wake of Prism, for instance, it is hard to imagine that special treatment and jurisdictional limitations on international data transfers – as a separate data processing activity – will not remain a key component of EU law. European sentiment toward its own version of privacy protection has quickly become far more entrenched. And yet, there are glimmers of hope. In the midst of August's revelations, you might have missed one release: announcing that IBM became the first company to be certified under the APEC cross-border privacy rules, a key focus of which is accountability for data flows as opposed to jurisdictional limitation.

Beyond the legislative wrangling, there is a danger that a loss of trust among national actors will somehow translate to the consumer and damage confidence in the digital medium. As long as companies keep their focus on the customer and customer choice, I believe there is little fear of that in the short term. As I spoke about in my podcasts in late July and early August, many companies – in the "big data" analytics space, for example – are doing their ablest to find the 'sweet spot' between 'killer app' and 'creepy app', particularly in the context of predictive search and applications (the New York Times and Forbes have each done excellent pieces on this). Others, like Stephen Balkam, try to turn our focus onto the "right to be forgiven" as opposed to "forgotten," and I commend his exceptional op-ed with regard to what that means. And still others, such as Forrester Research, see that privacy might be the next 'green movement', where companies will endeavor to compete on the basis of data practices. Every support to the economics of trust will be critical, for once trust is lost, it will be difficult to win it back.

Referring back to my experience in the Conor Pass – yes, sometimes, it's simply good not to know. And sometimes, knowing, you'd wish that you didn't and can put the known out of your mind. Then, there are times when it's vital to take in the maelstrom of events and environment and have these shape how you navigate the road ahead, warts and all. For privacy, and particularly the EU-U.S. experience, the last six months have been the latter. For privacy practitioners and professionals in the policy space, on both sides of the Atlantic, it's time to 'keep calm and carry on' – do your ablest to stay on the road.

Chris Boam is Founder and Principal of 40A&M LLC (http://40a-m.com/who-we-are.html) consulting.

Archive