Lines and Flows: The Beginning and End of Borders: Addendum I

Information sharing and personal data protection

Alan D Bersin[1]

The article, *Lines and Flows: The Beginning and End of Borders*,[2] posits in the contemporary security/trade context, that the logic of information sharing is irrefutable. It is now conceivable, indeed eminently executable, for a nation to check the identity of each passenger flying on every airplane, for example, toward its physical borders against "watch" lists of persons believed to pose a disproportionate security risk. Even though the receiving authority by definition would retain unfettered discretion to act on the information *vel non*, the record here, with a handful of exceptions, is that nations ostrich-like refuse regularly to avail themselves of access to this information. They do so in deliberate deference to other values which are deemed to be competing and of greater importance. Accordingly, these values are assigned a higher priority as matters of policy and practice. The Right to Privacy,[3] construed in one form or another, is the principal counter value interposed to the operational logic of information sharing for security purposes.

Traditionally both policymakers and the public have viewed individual privacy and national security as fundamentally at odds with one another, with policy questions preoccupied by the so-called trade-off of "so much security" for "so much abuse of civil liberties." This dichotomization has distracted the debate. Nations argue over the degree of primacy they give to privacy; they contend continuously over different definitions and types of privacy, as well as about alternative theories and models for implementing them. The debate, well worth the effort in its own terms, may turn out well beside the point in the contemporary context of information sharing.[4] There are two principal reasons supporting this conclusion.

First, the intersection between privacy protection and information sharing to enhance security in the global supply chain and global travel zones is crisp and sharp. One need not reconcile different visions, or points of departure concerning how to think about privacy,[5] in order to arrive at a common proposition regarding what steps are required to protect personal data in a specific case. At end, some application of *informed consent* can account for a satisfactory outcome. In other words, entry and engagement in global travel or supply chain activity embodies a bargain between public authorities and private actors. The contours of the bargain regarding use and dissemination have long been settled[6] once the threshold of *entitlement to collection* has been crossed.

In fact, upon closer observation, it appears that disagreements over data sharing – while argued as differences over privacy – usually reflect more a different assessment of the threat presented. Politically it is more convenient to decline information sharing based on asserted privacy concerns than it is to minimize risks of harm inherent in global trade and travel.

In short, there is no intrinsic conflict between security and privacy. The crucial policy challenge should be how both values can be advanced in tandem rather than balanced one against the other.

The second ground suggesting the compatibility between information sharing for security purposes and a robust respect for privacy relates to methods now available for sharing that avoid an actual *exchange* of data in favor of carefully tailored techniques of *access*.

Information-sharing is no longer a two-way exchange of data in which new information is incorporated or "dumped" in bulk form into a large-scale data base that is ever expanding with total availability and recall. Instead, modern information sharing compacts are predicated on the concepts of *federated search*. These are defined collectively (from *Wikipedia*) as… "an information retrieval technology that allows

the simultaneous search of multiple searchable sources: a user makes a single query request which is distributed to the search engines participating in the federation [and] the results received from the search engines [are aggregated in useful form] for presentation to the user."[7] The implications for the privacy/security discussion are dramatic.

First, there is no actual exchange of data at all as in the past. This obviates traditional concerns over subsequent use and disclosure. The scanning of data in place is conducted in a thoroughly masked fashion.

Second, the crucial agreement between authorities is embodied in the algorithms which implement the joint rule sets they stipulate. Access to the data is governed strictly by the nature of the query which may center on specific pre-identified risks or unknown threats identified by one or more agreed upon indicators. As Aaron Bady explains: "Pattern-based data mining… works in reverse from a subject-based search: instead of starting from known or strongly suspected criminal associations, the data miner attempts to divine individuals who match a data profile, drawing them out of a sea of data like the pattern in a color-blindness test."[8]

Third, the only information that actually is "shared" are the matches or "hits" that are returned from the federated search. These in turn are subject to negotiated protocols that treat the matches further to eliminate false positives and otherwise enhance security and privacy.

The federated search by its very nature is less intrusive than the old model of bulk data sharing: "It becomes more practical – and legally less complicated – to fish in an ocean of easily available information about everybody than to target specific suspicious individuals."[9] The argument, however, reaches further to the conclusion that the security regime itself is enhanced by building traditional considerations of privacy data protection into both the front and back ends of any information sharing arrangement. The twin dividends yielded from doing so are accuracy and efficiency resulting in an overall enhanced quality of result.

This approach incorporates key privacy concerns into the equation from the outset as measures of quality information assurance and control. Specifying what data are collected, who gets to use them and how, and the terms and conditions of dissemination and retention have significant potential to improve the end product from both security and privacy perspectives. These values become mutually reinforcing in theory as well as in practice within what Bady has characterized as a "very private pool of publicly circulating information."[10]

The privacy principles agreed upon by Canada and the United States in *Beyond the Border* [11]provide an important illustration of the kind of protections that should be built into a process to increase the *reliability* and *utility* of the process itself when data are accessed: purpose specification; relevance, necessity and proportion in light of clear purpose; accuracy and completeness; protection against risk such as loss, corruption, misuse, unauthorized access, alteration, disclosure, or destruction of data; accountability of governments involved overseen by a public supervisory authority; mechanisms to seek rectification and/or expungement of inaccurate personal information; transparency and notice on receipt and use of personal information; redress against infringement; parameters for transfer to third countries, and limits on data retention.[12]

Rejecting the scale of justice model as Homeland Security Secretary Janet Napolitano has advocated, creates the opportunity to make privacy and personal data protection concerns a central tenet in a security regime: "They are not a secondary part of the conversation [but rather] a fundamental part of [a single] conversation."[13] Exploring carefully the implications of this proposition can be expected to deliver operational insights beneficial to both values promoted over time in a sustained synthesis between security and civil liberty.

Notes

1 Reprinted with the permission of Alan D. Bersin, Assistant Secretary of International Affairs and Chief Diplomatic Officer, US Department of Homeland Security, Washington, DC.

2 Alan D. Bersin, *Lines and Flows: The Beginning and End of Borders*, Brooklyn Journal of International Law 2012, May, Vol. 37, No. 2, pp. 389-406; and World Customs Journal, Vol. 6, No. 1, pp. 115-126, March 2012.

3 Universal Declaration of Human Rights, Article 12; European Convention on Human Rights, Article 8; The (USA) Privacy Act of 1974, 5 U.S.C. s. 552ff.

4 See e.g. Mary Ellen Callahan and Wesley Wark, *Privacy and Information Sharing: The Search for an Intelligent Border, One Issue, Two Voices,* Woodrow Wilson International Center for Scholars, No. 13, October 2010.

5 Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. IV, No. 5, December 1890.

6 *Report of the Secretary's Advisory Committee on Automated Data System*, Commissioned by the U.S. Department of Health, Education, and Welfare: http://aspe.hhs.gov/DATACNCL/1973privacy/toprefacemembers.htm

7 See Peter Jacso, http://www2.hawaii.edu/~jacso, http://en.wikipedia.org/wiki/Federated_search

8 Aaron Bady, *World Without Walls*, online MIT Technology Review, November/December 2011. http://www.technologyreview.com/article/425905/world-without-walls/

9 Ibid.

10 Ibid.

11 Beyond the Border Action Plan: Statement of Privacy Principles by the United States and Canada, May 2012.

12 The Federal Trade Commission's Fair Information Practice Principles offer a comparable set of provisions: notice/awareness of disclosure; choice/consent for information to be used; access/participation to ensure the accuracy of personal data; integrity/security to prevent breaches; enforcement/redress in the event of a violation; self-regulation to create mechanisms for compliance; private remedies for consumers harmed by unfair information practices; government enforcement, and parental notice/awareness and parental choice/consent for disclosure of children's personal information.

13 Remarks by Secretary of Homeland Security Janet Napolitano: *Achieving Security and Privacy*, Australian National University, Canberra, Australia, May 3, 2011.

Alan D Bersin

Alan Bersin serves as Assistant Secretary for International Affairs and Chief Diplomatic Officer for the Department of Homeland Security where he oversees the Department's international engagement. Previously, he served as Commissioner of U.S. Customs and Border Protection. From April 2009 to March 2010 Mr Bersin served as Assistant Secretary for International Affairs and Special Representative for Border Affairs in the Department of Homeland Security.

Alan Bersin's other public service included Chairman of the San Diego County Regional Airport Authority (December 2006 to March 2009), California's Secretary of Education (July 2005 to December 2006) and Superintendent of Public Education in San Diego from 1998 to 2005. Mr Bersin also served as a member and then Chairman of the California Commission on Teacher Credentialing. From 1993 to 1998, he served as the United States Attorney for the Southern District of California and as the Attorney General's Southwest Border Representative responsible for coordinating federal law enforcement on the border from South Texas to Southern California. Mr Bersin previously was a senior partner in the Los Angeles law firm of Munger, Tolles & Olson.

In 1968, Mr Bersin received his A.B. in Government from Harvard University (magna cum laude). From 1969 to 1971, he attended Balliol College at Oxford University as a Rhodes Scholar. In 1974, he received his J.D. degree from the Yale Law School.