New International Privacy Principles for Law Enforcement and Security[1]

Mary Ellen Callahan, Chief Privacy Officer, U.S. Department of Homeland Security

Cross border data flows have long been a subject of global dialogue. In the late 1970s, the Organization for Economic Cooperation and Development (OECD) and the Council of Europe began exploring cross border transactions, with OECD issuing the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 and the Council of Europe issuing the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981. In 1990, the United Nations adopted the Guidelines for the Regulation of Computerized Personal Files. In 2004, the Asia Pacific Economic Cooperation issued its Privacy Framework. All four guidelines apply to the public sector, although they also include exemptions for law enforcement and security, which remain prevalent in national and European law.

Exemptions for law enforcement and security did not occur because of a dearth in sharing in this area nor for the desire to limit law enforcement cooperation, but were necessary to protect legitimate individual cases. Almost every country with the capability of doing so exchanges information on at least a case-by-case, if not routine, basis. None of these guidelines explicitly address exchanges between police working together on an investigation, which are guided by individual officers' application of domestic law. As a result, sharing between countries traditionally occurred on the basis of trust and mutual recognition, built on long-standing relationships between allies, or has been governed by broad cooperation agreements that give scant detail to privacy protections.

With the extensive increase in both international travel and security risks, there has been proportional growth in the need to share larger amounts of personal data for law enforcement and national security purposes. Data protection laws have also grown in complexity and sophistication. As a result, countries need to follow the lead of the private sector and provide greater transparency on privacy protections for data flows in the law enforcement and security context. Last month saw a landmark achievement in this area: U.S. and EU recognition of a set of core privacy principles for law enforcement and security.

The U.S.-EU High Level Contact Group

On October 28, officials representing the U.S. Departments of Homeland Security, Justice and State, together with the EU Presidency (represented by the Swedish Justice Minister) and the Vice President of the EU Commission, culminated almost three years of work by acknowledging the completion of the so-called High Level Contact Group (HLCG) principles. While the HLCG principles are not by themselves a binding agreement, this public acknowledgement reflects U.S.-EU shared values of democracy, rule of law, and respect for human rights and fundamental freedoms and the consequent commitment to effective data protection. These core principles will not only be the basis of future information sharing agreements between the EU and the U.S., but will hopefully raise the standard for information sharing in the law enforcement and security context for the rest of the world.

[1] As published in *The Privacy Advisor*, The Official Newsletter of the International Association of Privacy Professionals (IAPP), January 2010

There has long been an exchange of information between the EU member states and the U.S. for law enforcement and security purposes, resulting in numerous prosecutions. Most information sharing has occurred without controversy and without a single complaint of violation of the previously mentioned standards. However, the EU's growing authority in border and security matters vis-à-vis the member states changed the context of cooperation. The information sharing relationship with the U.S. appears to have become part of the evolving political dynamic between the EU and its member states. For example, the EU's Data Protection Framework Decision, adopted to protect privacy when European authorities share data among themselves, is prejudiced against the cooperation with non-EU partners. Likewise, the laws governing EU data systems for asylum seekers and border control (Eurodac and the Schengen Information System, respectively) restrict the transfer of data to third countries for legitimate law enforcement purposes. Unfortunately, in the name of protecting privacy, these restrictions negatively impact the equally legitimate activities of law enforcement to investigate and fight crime and terrorism.

The HLCG was formed in late 2006 to start discussions on privacy in the exchange of information for law enforcement purposes as part of a wider reflection between the EU and the U.S. on how best to prevent and fight terrorism and serious transnational crime. This group was composed of senior officials from the European Commission, the European Council Presidency and the U.S. Departments of Homeland Security, Justice and State. The goal of the HLCG was to explore ways that would enable the EU and the U.S. to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed. In October 2009, the group concluded the first step of that goal, producing a text that identifies the fundamentals or "common principles" of an effective regime for privacy. The next step will be for both sides to seek a binding international agreement.

The HLCG principles on privacy and personal data protection for law enforcement purposes applies in the EU for the prevention, detection, investigation, or prosecution of any criminal offense and in the U.S. for the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offenses or violations.

The HLCG data privacy principles include:

1. Purpose Specification/Purpose Limitation
2. Integrity/Data Quality
3. Relevant and Necessary/Proportionality
4. Information Security
5. Special Categories of Personal Information
6. Accountability
7. Independent an Effective Oversight
8. Individual Access and Rectification
9. Transparency and Notice
10. Redress
11. Automated Individual Decisions

12. Restrictions on onward transfers to third countries

Other HLCG principles addressed issues pertinent to the transatlantic relationship, including:

1. Private entities' obligations
2. Preventing undue impact on relations with third countries
3. Specific agreements relating to information exchanges
4. Issues related to the institutional framework of the EU and the U.S.
5. Equivalent and reciprocal application of data privacy law

The full text of the HLCG principles can be found at
http://useu.usmission.gov/Dossiers/Data_Privacy/Oct2809_SLCG_principles.asp

Implementation

Of course, identification of common principles and incorporation into a binding agreement do not end the obligations of the parties in providing privacy protection. As these principles are applied, the role of privacy authorities on both sides of the Atlantic will be to ensure that the relevant organizations are held accountable to them. Beyond a binding agreement, we may expect joint projects to include identification of best practices for ensuring accountability, such as assessments of decision-making frameworks for the collection and use of personal information, "privacy by design" tools, and privacy enhancing technologies (PETs). A practical, outcomes-driven focus would be a welcome contribution to law enforcement and security agencies throughout the world who adopt the HLCG principles.

****

Mary Ellen Callahan is the Chief Privacy Officer of the Department of Homeland Security; together with her colleagues from the Departments of Justice and State, she participated in the discussions related to the final HLCG principles. She wants to thank her International Privacy Policy Directors, Shannon Ballard and Lauren Saadat, for their assistance in the HLCG generally and with this article in particular.