Submission to the European Parliament
Committee on Civil Liberties, Justice, and Home Affairs

Hearing on the Reform of the EU Data Protection Framework:
Building Trust in a Digital and Global World

Session VII: Data Protection in the global context -
The transatlantic dimension

Bruce C. Swartz
October 10, 2012

Chairman Lopez Aguilar, Honorable Committee Members, Colleagues: I am pleased to have the opportunity to provide comments on the proposed EU data protection framework, and in particular how the draft Directive might affect law enforcement cooperation between EU Member States and third countries.

Over the past decades, crime has become unprecedentedly global in nature – and as a result the need for international law enforcement information sharing has become equally pressing. In 2006, a video showing a 10 year-old girl suffering sexual abuse was discovered by law enforcement in Australia. That discovery, followed by rapid, substantive information sharing among law enforcement, led to "Operation Koala" -- a multi-year, international investigation that eventually involved the law enforcement agencies of more than 28 countries, and revealed a child pornography website run by an Italian national, with material produced in the Ukraine, Belgium, the Netherlands and elsewhere. Operation Koala led to hundreds of arrests in countries around the world, and the identification of more than 30 child victims suffering sexual abuse. It succeeded only because of extensive law enforcement information sharing – the passage of personally-identifiable information regarding both suspects and victims – bilaterally and multilaterally, including through Eurojust, Europol, and INTERPOL.

Nor is "Operation Koala" unique. One need only glance at Eurojust's 2011 Annual Report to be reminded of the critical importance of transnational law enforcement information sharing. To cite but a few examples from that Report: A drug trafficking case – which Eurojust described as one of its "most complex" – involving Colombia, the U.S., Switzerland, Venezuela, Israel and Andorra, resulting in the arrest of more than 30 members of an organized crime group throughout the world. A tax fraud and money laundering investigation involving a network of companies in Panama, the Netherlands Antilles, and Switzerland. An alien smuggling ring led by Vietnamese nationals, linked to another criminal smuggling organization led by Iraqi Kurds. Sex tourism cases involving developing countries.

I begin by discussing "Operation Koala," and these other transnational investigations precisely because we are concerned that certain aspects of the Draft EU Data Protection Directive, if put into practice, could have a dramatic, and negative, effect on the ability to effectively share law enforcement information internationally in the future – thereby crippling international criminal investigations, and making citizens of EU Member States – and indeed citizens around the world – less safe. This is certainly not the intent of the Directive, or of anyone in this room, but let me mention a few of our concerns regarding the unintended consequences of the Directive.

First, Article 60 of the Directive states that "[i]nternational agreements concluded by Member States prior to the entry [into] force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive." This language seems to call into question hundreds of established, well functioning bilateral law enforcement related agreements and arrangements between EU Member States and third countries – including the United States -- as well as all existing multilateral law enforcement agreements -- including the

UNTOC, the UNCAC, the COE Cybercrime Convention, the 1988 UN Drug Convention, the UN counter-terrorism conventions – along with well established networks such as the Interpol system, the Egmont Group, and the 24/7 High Tech Crime Network.

It is our understanding that there is significant support among Member States for the principle that this Article should be revised or deleted, and that transfers to third countries pursuant to existing international agreements or other commitments should be unaffected or "grandfathered" into the directive. Such an amendment would be an important step. But I note that even if Article 60 is revised to "grandfather" in prior international agreements, the Directive as currently drafted still would call into doubt the ability of EU Member States to enter into any future multilateral law enforcement agreements. Over the past decade, in response to the globalization of crime, EU Member States, the United States, and other countries have built an international legal regime that calls for providing mutual legal assistance in criminal and terrorism matters to the maximum extent possible – language that is embedded in the UN and COE Conventions. To quote from the explanatory report of the Budapest Convention against Cybercrime: "grounds for refusal . . . should be narrow and exercised with restraint. They may not be so expansive as to create the potential for assistance to be categorically denied, or subjected to onerous conditions, with respect to broad categories of evidence or information."

But it is precisely that type of categorical denial that the Directive puts in place. This brings me to our second concern with the provisions of the Directive. Chapter V of the proposed directive, which relates to the transfer of personal data to third countries or international organizations, provides that an "adequacy" decision by the Commission is the primary means to maintain the broad cooperation that currently exists. As drafted, the criteria to be considered by the Commission in making such an "adequacy" determination would include comparisons to a

European style system of data protection. Absent an adequacy finding, Member States may share information broadly only if "appropriate safeguards" are in place with the receiving country, through a binding agreement or otherwise. But how that determination would be made is unclear. And should neither an "adequacy" nor "appropriate safeguards" finding be in place, it appears that transfer is permitted only by way of a case-by-case "derogation," and is subject to reversal by data protection officials, the foreseeable result of which would be a significant reduction in and slowing of cooperation and a substantial increase in resources needed to address these issues.

This in turn raises a third concern: we read the proposed Directive to provide the power to data protection officials to make the ultimate decisions on whether and to what extent Member States may provide international cooperation in law enforcement matters. In this regard, we are concerned that national investigating and prosecuting officials, and Justice and Interior Ministry experts, would not have the final word on the issue of providing cooperation. For example, Article 46 of the proposed Directive (together with Articles 25 and 30) requires the Member States to facilitate the review of data transfers by data protection officials, and gives those officials the ability to "impose a temporary or definitive ban on processing" of personal data -- in other words, the power to order the police, investigators and prosecutors to stop sharing information with a third country. Thus, the Directive would give data protection officials the authority to reverse the determination of Member States investigative, prosecutorial, and international cooperation officials that it is appropriate under the rules of international cooperation to provide information important to protecting their citizens, or the citizens of another State.

Our fourth concern is that Article 54 provides that individual processors -- such as police officers, investigators or prosecutors -- "shall be jointly and severally liable" for "actions incompatible with" the Directive. The proposed Directive contains no requirement for a specific mental state in this regard, e.g., intentional, reckless or grossly negligent violations. Rather, the standard appears to be strict liability, which causes us significant concern, particularly in view of the complexity of the Directive's text in many respects. Our experience is that law enforcement officials, if they believe there is even a small chance of individual liability, will be reluctant to share information. Thus, these provisions give rise to the risk of chilling, in some cases potentially with tragic effect, our information sharing.

I would also like to turn for a moment to related issues with regard to the proposed Regulation. I note that although the Regulation expressly excludes from its scope exchanges between justice and security sector officials, it still appears to have an impact on the law enforcement functions of non-EU states – and we would urge this also be considered. By way of example, we are studying the extent to which it brings within its scope, and thereby subjects to EU law, the activities of regulatory agencies of third countries that are that are closely linked to law enforcement functions -- such as arms and controlled substance import regulations administered by the U.S. Department of Justice -- as well as other regulatory functions, such as those carried out by banking and securities regulators, whose enforcement investigations can culminate in criminal investigations and prosecutions, and whose record-keeping requirements facilitate our ability to obtain crucial evidence for many kinds of criminal cases. We wish in all events to avoid a potential conflict of laws with respect to the ability of regulatory agencies to assist law enforcement efforts.

Let me conclude by expressing the hope that the data privacy framework will maintain the vitality of the current system for international cooperation against transnational crime and terrorism. Over the past decades, the EU and the EU Member States have been in forefront in creating that system of international cooperation – and if we are to protect our citizens, we cannot afford to let it be weakened. It is because of the importance of this issue – which goes far beyond our bilateral relations -- that we are particularly grateful for this opportunity to discuss the draft data protection framework. I would respectfully ask the Commission and the Parliament to continue to engage with us in a regular discussion of the development of these instruments as they progress, so that we can provide our perspectives as a third country that has deep cooperation with the European Union, and shares the same values.

Thank you very much for having given me the opportunity to address you today on these important issues.