EU and U.S. privacy proposals converge on principles, diverge on method

Privacy has never mattered as much as it does today. In an era of rapidly-evolving technology capable of collecting, storing, sharing (and potentially, mishandling) personal data about every aspect of our lives, the privacy stakes are high. And with almost daily headlines about privacy abuses and mistakes, it is not surprising that policymakers around the world are re-examining the legal frameworks in place to protect personal privacy.

The privacy problem is not restricted to any one jurisdiction. The problem is a global one. The Internet, social media and Cloud computing cross national borders. Indeed, the wonder of modern technology is the ability of people to access information and entertainment from virtually anywhere, and to send information globally. Thus, one would expect nations of the world to come together to propose a global standard of protection.

In that connection, at a recent conference held simultaneously in Washington and in Brussels, the EU's Minister of Justice and the U.S. Secretary of Commerce issued a joint statement declaring that "This is a defining moment for global personal data protection and privacy policy and for achieving further interoperability of our systems on a high level of protection."

One basis for the hoped-for interoperability is the wide agreement around the world, as there has been for decades, on the basics of what it means to protect privacy in an information age. The so-called "Fair Information Practice Principles," or "FIPPs", focus on empowerment of people to control their personal information and on safeguards to ensure adequate data security. FIPPs form the core of the 1980 OECD privacy guidelines on which both the U.S. and European models are based.

But, historically, the EU and U.S. have taken divergent approaches to implementing the FIPPs. In the U.S., where privacy interests are balanced with the right to free expression and commerce, and in recognition of the fact that – as a practical matter – not every piece of personal information can be protected and policed, the framework provides highest levels of protection for sensitive personal information, such as financial, health and children's data. In addition, targeted enforcement actions against bad (or negligent) actors– principally by the U.S. Federal Trade Commission – have created a "common law" of what is expected from business when it comes to the collection, use and protection of personal information. In addition, Chief Privacy Officers are proliferating and gaining in importance in U.S. businesses, adding to the level of American privacy protection. Data security breach notification laws are credited with creating a negative incentive for businesses to buttress the protection of personal data (to avoid having to report breaches to regulators and to the public).

In the EU, by contrast, a region-wide Directive, with national laws in 27 jurisdictions to implement the requirements of the Directive, purports to regulate every piece of personal information, and is predicated on the notion that privacy is a fundamental human right. Thus, under the approach of across-the-board regulation, there are strict limits on the collection and use of information, although enforcement of those limits has been episodic. Some of the enforcement actions have been criticized, such as the criminal case against Google executives for the posting by a YouTube user of a video showing an invasion of privacy – a video that Google took down when notified about it

Still, the EU firmly believes its framework is superior to that of the U.S., and it has been steadfast in the belief that because the U.S. does not have an across-the-board privacy law, its protections are inadequate and transfers of personal data from the EU to the U.S. must be controlled and subject to special regulation.

Is 2012 a time for hope that the tensions between the EU and the U.S. over their respective approaches to privacy will subside? Will the fact that both jurisdictions are working to revise their privacy frameworks mean that there will be convergence and greater cooperation?

.

In January, the European Commission unveiled its bold new vision for privacy in the EU, calling for a region-wide Regulation to sweep away the inconsistencies of national laws passed to implement the 1995 Directive on Data Protection and proposing strict new privacy rules (and penalties for violating those rules). The proposed rules are intended to take into account the pervasive new technologies capable of collecting and sharing information about people, and to give individuals more control over their personal information. One month later, in the United States, the Obama Administration announced its "Privacy Blueprint" for the United States, calling for legislation containing a Privacy Bill of Rights and proposing enforceable codes of conduct developed through a so-called "Multi-stakeholder Process." The independent U.S. Federal Trade Commission followed shortly thereafter with a report on privacy containing that agency's expectations and hopes for the collection of personal information.

There are indeed common aspects to the EU and U.S. proposals. Both call for implementation of the "Privacy by Design" concept intended to build in privacy sensitivity and consideration into every stage of the development of products and services. Both recognize the importance of accountability by those who collect and use personal data. Both reflect the principle that people should not be surprised by the use of their personal data collected for one purpose but used for another purpose. There is no disagreement about the need for informed consent about the collection and use of personal information (although the kind of consent envisioned in each place differs as to various categories of data).

Big differences in approach emerge from the fact the U.S., while proposing a first-ever federal privacy law with a "Privacy Bill of Rights," still intends to rely on a variety of self-regulation (more precisely, co-regulation since self-regulatory rules could enforced by law enforcement). And the U.S. proposed rules do not contemplate a "right to be forgotten," a major feature of the EU proposal and one that First Amendment scholar Professor Jeffrey Rosen has labeled "the biggest threat to free speech on the Internet in the coming decade." Similarly, there is no right to "data portability" in the U.S. proposals as there is in the EU plan. The EU proposal contemplates broad jurisdiction to enforce its law, even to U.S. businesses without a physical presence in the EU, under certain circumstances. And even though the EU has borrowed the data breach notification idea from the U.S., it proposes a presumptive obligation to provide notice within 24 hours of a breach, a time frame widely regarded as wholly unworkable by those who have worked under the U.S. data breach laws. Finally, the EU proposes a schedule of monetary fines of up to 2% of an entity's global world-wide turnover for violations of the proposed Regulation – an amount viewed as wildly unreasonable in light of the potential for abuse by enforcers. In January, the European Commission unveiled its bold new vision for privacy in the EU, calling for a region-wide Regulation to sweep away the inconsistencies of national laws passed to implement the 1995 Directive on Data Protection and proposing strict new privacy rules (and penalties for violating those rules). The proposed rules are intended to take into account the pervasive new technologies capable of collecting and sharing information about people, and to give individuals more control over their personal information. One month later, in the United States, the Obama Administration announced its "Privacy Blueprint" for the United States, calling for legislation containing a Privacy Bill of Rights and proposing enforceable codes of conduct developed through a so-called "Multi-stakeholder Process." The independent U.S. Federal Trade Commission followed shortly thereafter with a report on privacy containing that agency's expectations and hopes for the collection of personal information.

There are indeed common aspects to the EU and U.S. proposals. Both call for implementation of the "Privacy by Design" concept intended to build in privacy sensitivity and consideration into every stage of the development of products and services. Both recognize the importance of accountability by those who collect and use personal data. Both reflect the principle that people should not be surprised by the use of their personal data collected for one purpose but used for another purpose. There is no disagreement about the need for informed consent about the collection and use of personal information

(although the kind of consent envisioned in each place differs as to various categories of data).

Big differences in approach emerge from the fact the U.S., while proposing a first-ever federal privacy law with a "Privacy Bill of Rights," still intends to rely on a variety of self-regulation (more precisely, co-regulation since self-regulatory rules could enforced by law enforcement). And the U.S. proposed rules do not contemplate a "right to be forgotten," a major feature of the EU proposal and one that First Amendment scholar Professor Jeffrey Rosen has labeled "the biggest threat to free speech on the Internet in the coming decade." Similarly, there is no right to "data portability" in the U.S. proposals as there is in the EU plan. The EU proposal contemplates broad jurisdiction to enforce its law, even to U.S. businesses without a physical presence in the EU, under certain circumstances. And even though the EU has borrowed the data breach notification idea from the U.S., it proposes a presumptive obligation to provide notice within 24 hours of a breach, a time frame widely regarded as wholly unworkable by those who have worked under the U.S. data breach laws. Finally, the EU proposes a schedule of monetary fines of up to 2% of an entity's global world-wide turnover for violations of the proposed Regulation – an amount viewed as wildly unreasonable in light of the potential for abuse by enforcers.

Christopher Wolf
T +1 202 637 8834
christopher.wolf@hoganlovells.com

Winston Maxwell
T +33 (1) 5367 4847
winston.maxwell@hoganlovells.com

The period ahead will be one for adjustments to the proposed EU Regulation to make it acceptable to the European Parliament and to the Council of the European Union, the bodies responsible for the co-decisioning process required to adopt the Regulation. Input can be expected from businesses in Europe concerned about the practicality and the effect on trade of the proposed more-restrictive privacy rules. Likewise, in the U.S., the exact shape of the new privacy framework is still to be determined, on Capitol Hill and through the work of the Executive Branch.

But as things now stand, there is a big gap to bridge between the two trans-Atlantic approaches. In many ways, so close. Yet, very far apart in fundamental respects.

"the right to be forgotten is the biggest threat to free speech on the internet in the coming decade."

"... a defining moment for global personal data protection."