37TH International Privacy Conference Amsterdam 2015

PRIVACY BRIDGES

EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS

PRIVACY BRIDGES

EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS

AMSTERDAM / CAMBRIDGE
SEPTEMBER 2015

PROJECT PARTICIPANTS

Jean-François Abramatic	French National Institute for Computer Science and Applied Mathematics
Bojana Bellamy	Centre for Information Policy Leadership at Hunton & Williams
Mary Ellen Callahan	Jenner & Block
Fred Cate	Indiana University Maurer School of Law
Patrick van Eecke	University of Antwerp
Nico van Eijk	Institute for Information Law (IViR) University of Amsterdam (UvA) (Co-chair)
Elspeth Guild	Centre for European Policy Studies
Paul de Hert	Vrije Universiteit Brussel (VuB) and Tilburg University
Peter Hustinx	European Data Protection Supervisor (EDPS) (retired)[1]
Christopher Kuner	Vrije Universiteit Brussel (VuB)
Deirdre Mulligan	University of California Berkeley
Nuala O'Connor	Center for Democracy and Technology
Joel Reidenberg	Fordham University School of Law
Ira Rubinstein	Information Law Institute, New York University School of Law (Rapporteur)
Peter Schaar	European Academy for Freedom of Information and Data Protection
Nigel Shadbolt	University of Oxford
Sarah Spiekermann	Vienna University of Economics and Business (WU Vienna)
David Vladeck	Georgetown University Law Center
Daniel J. Weitzner	Massachusetts Institute of Technology (Co-chair)

OBSERVER

Jacob Kohnstamm	Dutch Data Protection Authority (CBP)

PROJECT SUPPORT

Frederik Zuiderveen Borgesius	Institute for Information Law (IViR) University of Amsterdam (UvA)
Dominique Hagenauw	Dutch Data Protection Authority (CBP)
Hielke Hijmans	Vrije Universiteit Brussel and University of Amsterdam (UvA)

The project support staff actively participated in the preparations and discussions of the Report.

[1] *Until December 2014 Peter Hustinx participated as an observer*

EXECUTIVE SUMMARY

Globalization and technological advances pose common challenges to providing a progressive, sustainable model for protecting privacy in the global Internet environment. Tensions between different legal systems such as the European Union and the United States result in loss of confidence on the part of users and confusions by commercial entities. The goal of this report is to identify practical steps to bridge gaps between the existing approaches to data privacy of the European Union (EU) and the United States (US), in a way that produces a high level of protection, furthering the interests of individuals and increasing certainty for commercial organizations. These "privacy bridges" are designed to advance strong privacy values in a manner that respects the substantive and procedural differences between the two jurisdictions. While our focus is privacy protection in the transatlantic region, we hope that some, if not most, of these privacy bridges may prove useful in other regions as well.

This report emerged from a series of in-person meetings and discussions among a group of independent EU and US experts in the field of privacy and data protection. This group was convened on the initiative of Jacob Kohnstamm, chairman of the Dutch Data Protection Authority, and jointly organized by the Massachusetts Institute of Technology Cybersecurity and Internet Policy Research Initiative, and the University of Amsterdam's Institute for Information Law.

We present ten privacy bridges that will both foster stronger transatlantic collaboration and advance privacy protection for individuals.

BRIDGE 1

DEEPEN THE ART. 29 WORKING PARTY/FEDERAL TRADE COMMISSION RELATIONSHIP

The Article 29 Working Party (WP) (as leading representative of the EU Data Protection Authorities) and the United States Federal Trade Commission (FTC) should commit to regular, public dialogue and policy coordination on leading privacy challenges faced in the transatlantic region. This bridge would institutionalize the working relationship between the Article 29 WP and the FTC via a Memorandum of Understanding (MOU). This MOU will foster better cooperation and more efficient policy development and enforcement by these regulators, thereby delivering enhanced privacy protection to individuals on both sides of the Atlantic.

BRIDGE 2

USER CONTROLS

Users around the world struggle for control over their personal information. This bridge calls on technology companies, privacy regulators, industry organizations, privacy scholars, civil society groups and technical standards bodies to come together to develop easy-to-use mechanisms for expressing individual decisions regarding user choice and consent. The outcome should be usable technology, developed in an open standards-setting process, combined with clear regulatory guidance from both EU and US regulators resulting in enhanced user control over how data about them is collected and used.

BRIDGE 3

NEW APPROACHES TO TRANSPARENCY

This bridge recommends that the Article 29 WP and the FTC rely on the MOU described in Bridge 1 to coordinate their recommendations on privacy notices and then jointly encourage an international standardization process. By pooling the insights that they gained from earlier and ongoing standardization efforts, and drawing on lessons learned by other industries on required notifications (e.g. nutrition labeling), they can develop more definitive guidance on transparency and thereby achieve a necessary condition for the user controls described in Bridge 2.

BRIDGE 4

USER-COMPLAINT MECHANISMS: REDRESS OF VIOLATIONS OUTSIDE A USER'S REGION

Users interact with web-based services from all around the world. When they have complaints, they should have an easy path to resolution. This bridge encourages all online services to provide contact information and calls upon the appropriate EU and US public agencies to cooperate on the creation of a directory of basic information about relevant jurisdictions and how and to whom complaints concerning data privacy may be brought.

BRIDGE 5

GOVERNMENT ACCESS TO PRIVATE SECTOR PERSONAL DATA

This bridge offers guidance to, in particular, telecommunication and Internet services faced with surveillance from their own and foreign governments. Specifically, it recommends that all such companies establish uniform internal practices for handling such requests regardless of jurisdiction, citizenship, and data location; report on practices relating to government access requests on a regular basis; and adopt best practices based on international standards (such as those of the Global Network Initiative), with the goal of developing a framework for assessing and responding to requests for data originating outside national territory.

BRIDGE 6

BEST PRACTICES FOR DE-IDENTIFICATION OF PERSONAL DATA

De-identification of personal data is a critical tool for protecting personal information from abuse. This bridge calls on EU and US regulators, who already share common views about de-identification, to identify concrete, shared standards on de-identification practices. Common standards will improve privacy protections on both sides of the Atlantic while enhancing legal certainty for both EU and US organizations that follow these recommendations.

BRIDGE 7

BEST PRACTICES FOR SECURITY BREACH NOTIFICATION

Although information security breaches have a global impact on users given that many of them reside in different jurisdictions than those of service providers, there is lack of uniformity in security breach notification laws, both domestically (across distinct sectors) and even more so internationally. This bridge recommends that the relevant authorities cooperate when dealing with multi-nation breaches, both in terms of enforcement and in establishing a more harmonized breach-reporting regime. It also recommends that firms complement their reporting obligations by adopting robust information governance systems, which should result in an increase in the level of privacy protection of end users.

BRIDGE 8

ACCOUNTABILITY

Both EU and US regulators have accepted the idea of organizational responsibility (or "accountability") as a means to assure data protection and for firms to satisfy domestic legal obligations. This bridge identifies the common elements of enforceable corporate accountability programs. It recommends that the Article 29 WP and FTC harmonize their approaches while emphasizing the need for the private sector to develop more effective means for external verification and scaling of accountability programs for use by small and medium enterprises. The hoped for outcome is an improvement in actual data processing practices that not only benefits individuals but also offers companies more effective compliance guidelines for international operations.

BRIDGE 9

GREATER GOVERNMENT-TO-GOVERNMENT ENGAGEMENT

This bridge proposes that in parallel with the MOU suggested in Bridge 1, European and US executive agencies and decision-making bodies engage in active dialogue and, where appropriate, effective coordination of their regulatory activity. Such government-to-government engagement seems especially valuable in a number of new sectors in the transatlantic economy (an interesting example is the development and use of drones) that pose acute privacy challenges. The exchange of information on a regular basis and development of transparent platforms for active discussion and practical policy development will yield a variety of benefits to governments, individuals, and commercial actors alike.

BRIDGE 10

COLLABORATING ON PRIVACY RESEARCH PROGRAMS

Finally, this bridge encourages the growth of common perspectives on privacy in the EU and US by fostering collaborative, multidisciplinary engagement of privacy researchers on both sides of the Atlantic. It identifies barriers to bringing together academics to work on joint privacy research projects in a variety of fields and suggests ways to overcome them.

These ten privacy bridges are all practical steps that require no change to the law yet will result in better-informed, and more consistent, regulatory cooperation, policy guidance, and enforcement activity. Our mandate as a group is to produce recommendations that can be acted upon without changes in the legislative environment of either the EU or US. While many members of the expert group that produced these recommendations have strong views about the future direction of US and EU privacy laws, here we seek to surmount privacy challenges facing the information society, without entering into divisive debates on changes to underlying constitutional or statutory frameworks. Changing the law is an arduous and lengthy endeavor, and waiting for it to happen can become simply an excuse for inaction. Ideally, this report will bring about improvements in privacy protection due to positive actions not only by governments and regulatory authorities, but also by the private sector, civil society, and others, all of whom may implement its recommendations.