37TH International Privacy Conference Amsterdam 2015

# PRIVACY BRIDGES

EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS



Institutional support for this project was provided by the Massachusetts Institute for Technology Computer Science and Artificial Intelligence Laboratory (Cambridge, MA – United States) and the Institute for Information Law of the University of Amsterdam (Amsterdam – the Netherlands).
https://privacybridges.mit.edu/

# 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.

# TABLE OF CONTENTS

# I. INTRODUCTION

## A. TRANSATLANTIC PRIVACY CHALLENGES IN A GLOBALIZED WORLD

In recent years there has been a huge growth in the complexity and volume of global data flows and data processing. More information is available than ever before. There are over 3 billion Internet users worldwide and they use and enjoy thousands of online services and hundreds of thousands of apps. Never in human history has it been so easy for people to communicate and exchange information regardless of their location or situation. All of these trends have brought countless social and economic benefits.

However, these same developments have also created new threats to privacy. Individuals are concerned by the lack of transparency with regard to how their personal data are processed, and they are frustrated by a lack of control over such data. Companies capture, store, manage, and analyze data on a massive scale, and often fail to respect the data privacy rights of individuals. In the predominant online advertising business model, companies deliver "free" products or services and receive revenue from advertisers. And those companies that rely on behavioral advertising select and display ads based on highly detailed user profiles, which only intensifies the collection and sharing of personal data. As much as Internet users benefit from free content, they also have an abiding feeling of distrust in how most online companies use their personal information.

Government agencies also collect and process massive amounts of data for legitimate government purposes, ranging from the provision of services to law enforcement and national security functions. The Snowden and other revelations, however, suggest that online data are being processed by the intelligence services of numerous countries with a lack of adequate legal controls, and that governments are increasingly accessing data originally collected by private sector firms. The law and traditional forms of regulation often struggle to restrain these excesses.

Globalization and technological advances also pose privacy challenges. To give just a few examples, the gigantic network of physical objects embedded with electronic sensors, and connectivity (the so-called Internet of Things) and the broad range of new data types and massive data sets (so-called Big Data) raise a host of unanswered questions about how to apply established privacy values to new technological platforms. Moreover, new decentralized market structures and business relationships (such as the countless independent apps running on global platforms) raise questions about the scope and adequacy of enforcement efforts. Given the global reach of these developments, there are common challenges of providing a progressive, sustainable model for privacy rules in the global Internet environment.

The above phenomena, both positive and negative, are global in nature and not limited to any particular region. However, the European Union (EU)[2] and the United States of America (US) have

[2] *Throughout this Report, references to the "EU" include both the institutions of the European Union and the EU Member States, which include Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.*

close historical and social ties, a common tradition of upholding human rights, and a significant economic relationship. The EU and US work closely with many other leading regions and countries that have developed their own approaches to privacy.[3] As such, the way that the EU and the US protect privacy is closely watched around the world, and can influence developments in other regions.

The last few years have seen an increasing number of divergences between the EU and the US with regard to privacy, covering areas such as the efficacy of regulatory protections, the data processing practices of companies, and foreign intelligence surveillance. Too often the resulting tensions have been as much about scoring political points as about substantive issues. We believe it is crucial to emphasize instead what the two sides have in common by identifying practical measures to increase privacy protection that could be used both in the transatlantic setting and potentially in other regions around the world.

## B. SCOPE AND PURPOSE OF THE PRIVACY BRIDGES GROUP

The Privacy Bridges group was established to identify a framework of practical measures to advance strong privacy values in a manner that respects the substantive and procedural differences between the EU and the US. Besides stimulating discussion and encouraging greater convergence, it is hoped that this Report can lead to action by governments, regulatory authorities, the private sector, civil society, and others to implement its recommendations.

The EU and the US share a common heritage in their views on democracy, the rule of law, and fundamental freedoms. Both address privacy from similar foundations, based on principles of autonomy, dignity and restraint on government power. They have many common interests, including increasing the transparency of data processing on the Internet, facilitating the assertion of privacy rights by individuals, and restraining government surveillance. There has been cooperation between the EU and the US on privacy issues (such as in the drafting of the 1980 and 2013 versions of the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) and cross-fertilization between their regulatory approaches since the 1970s). They also have a common interest in resisting worrisome trends that are emerging in other regions, such as the restriction of free speech online, data localization, and – in some regions - fragmentation of the Internet.

Our goal is to identify a few selected practical steps to bridge gaps between the existing EU and US approaches to data privacy, in a way that produces a high level of protection and furthers the interests of individuals. These "privacy bridges" are designed to advance strong privacy values in a manner that respects the substantive and procedural differences between the two jurisdictions.

Privacy bridges are practical step that requires no change to the law and that results in better-informed, and more consistent, regulatory cooperation, policy guidance, and enforcement activity. This paper contains a non-exhaustive list of privacy bridges that, in our opinion, both foster stronger collaboration between the EU and US and advance privacy protection for individuals. While our focus is privacy protection in the transatlantic region, we hope that some of these privacy bridges may prove useful in other regions as well.

---

[3] *These include the 21-member Asia-Pacific Economic Cooperation (APEC) and individual countries such as Argentina, Australia, Canada, Hong Kong, Israel, Japan, New Zealand, and South Korea.*

Implementing our proposals requires attention to the differing governmental structures of the EU and the US. The EU is an autonomous legal entity to which its 28 Member States have ceded part of their sovereignty, while the US is a federal republic comprised of 50 states. It is for the EU and the US to best decide how to provide for privacy protections within their own democratic frameworks. However, we believe that particularly with regard to online issues, there is a need for greater global cooperation in order to provide better protection of privacy.

It is also important to state clearly what this project does not cover. In accordance with our self-imposed mandate, we accept as a given the current legal frameworks in the EU and the US. Thus, we take no position on the need to change the law (besides a few suggested changes to administrative rules in the context of improving regulatory cooperation, and some comments regarding national intelligence surveillance). We believe that such discussions are best left to governments and other public institutions that can debate and resolve these issues in a democratic, accountable fashion. We also believe that there is already much discussion about legal issues, and what has been missing has been the identification of practical solutions to help bridge gaps between the two systems.

We have only considered privacy bridges that meet three criteria. First of all, they must involve practical steps that can be taken by defined actors within a reasonable time period. Second, they must not involve changes to constitutional principles or to the law (besides the two exceptions noted above). Finally, they must have a positive effect on the level of privacy protection on both sides of the Atlantic.

There is no widely accepted definition of the term "privacy", and in EU law there is a distinction between "privacy" and "data protection". By contrast, in the US the protection of an individual's "private space", the collection and use of "personally identifying information", and other related topics tend to be subsumed under the term "privacy". This is an example of using the same terms to mean different things that is one of the causes of misunderstandings between the two sides.

For reasons of convenience, we use the term "privacy" throughout this Report to refer broadly to the interest that individuals have in restricting the processing of data related to themselves. Hence, this term includes concepts such as privacy, data protection, and "data privacy". Privacy so understood is also protected in international human rights instruments such as Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). However, we do not deal with related issues that are peripheral to the concept of data privacy, such as the protection of reputation, regulation of the media, or the legal protection of confidentiality.

Finally, many individuals are seriously concerned about data processing by governments for intelligence gathering and law enforcement purposes. Dealing in detail with these topics would require making suggestions for changes in the law, and thus falls outside our mandate. However, all members of the group are concerned about the practices of a number of countries brought to light by the Snowden and other revelations, and do not believe that they can be neatly separated from private-sector issues. Thus, we have not hesitated to refer to issues raised by intelligence surveillance and law enforcement practices where this is relevant.

In summary, the purpose of the group is to promote the adoption of practical solutions on both sides of the Atlantic, in order to surmount privacy challenges facing the information society, without entering into divisive debates on changes to the underlying constitutional or statutory framework.

## C. PROJECT PARTICIPANTS AND ORGANIZATION

The group was convened on the initiative of Jacob Kohnstamm, chairman of the Dutch Data Protection Authority and former chair of the Article 29 Working Party (the group of EU Data Protection Authorities (DPAs)). The project has been jointly organized by the Massachusetts Institute of Technology Cybersecurity and Internet Policy Research Initiative, USA, and the Institute for Information Law (IViR) of the University of Amsterdam, The Netherlands. This Report will be presented at the 2015 International Conference of Privacy and Data Protection Commissioners, which the Dutch Data Protection Authority will host in Amsterdam on 28-29 October 2015.

The members of the group are independent experts in the field of privacy and data protection from the European Union and the United States. They include individuals with decades of experience working on privacy-related issues in academia, data protection authorities, government agencies, business, and legal practice. The criterion of independence means that the experts are not employees of corporations or public authorities, that in their work they do not favor a specific national or business interest, and that they all participate in a personal capacity, free from political influence. A small number of persons (including Mr. Kohnstamm) have only participated as observers. Annex 1 contains short biographies of the members of the group. The academic and government institutions listed in Annex II pay the travel, administrative, and support costs related to the meetings, but no member of the group has received any remuneration for participating. The group is organized on an informal basis, and has no pre-determined political commitments.

This Report was drafted in the course of several meetings held in 2014-2015 in the EU and the US, during which the group heard presentations from representatives of government, business, civil society, and academia. A complete list of the meetings and the organizations that gave presentations to the group – insofar as they agreed to be mentioned – is contained in Annex III.

The views of the group's members on the merits of the respective EU and US approaches to privacy protection differ widely. But we are in agreement that the public discussion has largely overlooked the progress that may be achieved when taking a broader view and building on what these two approaches have in common rather than focusing on their differences.

# II. PRIVACY PROTECTION IN THE EU AND THE US

The systems of privacy protection in the EU and the US have common roots, and evidence both similarities and differences, which are important as background for the privacy bridges we propose. The following are brief overviews of both systems, which we have drafted in an objective and non-partisan fashion. We are aware that initiatives to review and/or adopt legislation are underway on both sides of the Atlantic, which have been taken into account in the discussion below.

## A. PRIVACY PROTECTION IN THE EU

Within the EU, privacy and data protection are laid down as fundamental rights on a constitutional level, in the Treaty on the Functioning of the EU (which entered into force in 2009 as part of the so-called "Treaty of Lisbon") and in the Charter of the Fundamental Rights of the EU (EU Charter). The main elements of protection are laid down in these basic legal instruments, including the enforcement of protection by independent agencies. Many constitutions of EU Member States contain similar rights.

The Court of Justice of the European Union (CJEU), which is the highest court in the EU, has also repeatedly emphasized the fundamental rights to privacy and data protection in its judgments. Constitutional and fundamental rights of privacy in the EU may be "positive" as well as "negative", i.e., they may compel that government action be taken as well as requiring that it not be taken, and may thus provide protection against intrusions both in the public and in the private sector. This may involve secondary legislation setting out further details.

The idea of privacy in Europe derives from concepts such as human dignity and the rule of law. Modern conceptions of privacy began to develop following the experiences of fascism in World War II and communism in the post-war period. There is a distinction in European law between "privacy" and "data protection" – the two concepts are closely related, and often overlap, but are not synonymous. Privacy generally refers to protection of an individual's "personal space", while data protection refers to limitations or conditions on the processing of data relating to an identifiable individual.

In 1949 the countries of Europe formed an international organization called the Council of Europe (CoE), which is distinct from the EU. In 1950 the CoE adopted the European Convention on Human Rights (ECHR), an international treaty that has been adopted by all 47 CoE member states (including all 28 Member States of the European Union). The European Court of Human Rights enforces the Convention. Article 8 of the Convention protects private and family life, which the Court of Human Rights has interpreted to include the protection of the processing of personal data. The CoE has also promulgated a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), another international treaty that specifically covers data protection and is force in 46 states.

The main legal instrument in the EU with regard to data privacy is the EU Data Protection Directive 95/46 (the Data Protection Directive), which came into force in 1998 and covers the processing of

personal data in both the private and public sectors. It gives further effect to Convention 108 in the EU Member States, and aims in particular both to create a high level of data protection throughout the EU, and to enable a free flow of information within the EU's internal market. The Data Protection Directive is based on a few overriding principles such as legitimacy, purpose limitation, transparency, proportionality, security, and control by an independent supervisory authority. The Data Protection Directive requires Member States to ensure that their national law adheres to its principles, but its interpretation throughout the EU reflects national differences and is not homogenous.

The Directive also permits data transfers to countries outside the EU only if the applicable laws in the receiving country guarantee an "adequate level of data protection". A decision issued by the European Commission provides that adequate protection exists for transfers covered by the Safe Harbor, which is a self-regulatory scheme that US-based companies can join and can be enforced by the US Federal Trade Commission. The Safe Harbor has been instrumental in introducing many US companies to EU data protection law. But it has also been subject to criticism in the EU, and is currently subject to a legal challenge before the CJEU. Some of the other major legal bases allowing for the international transfer of personal data include the consent of the individual; the conclusion of standard contractual clauses between the data importer and data exporter; and the use of binding internal policies (so-called "Binding Corporate Rules" or BCRs) among the entities of a particular corporate group. The EU has also concluded bilateral agreements with the US that contain privacy protections for certain types of data accessed by the US authorities for law enforcement purposes (e.g. airlines passenger name record data and certain financial messaging data).

The Data Protection Directive includes a broad exemption for law enforcement and national intelligence activities, although they are covered by the ECHR and by specific legislation. The level of harmonization of data protection relating to law enforcement authorities is less comprehensive, but there is a general EU instrument (Data Protection Framework Decision) and there are sector specific rules. Jurisdiction over intelligence activities is generally reserved for the Member States, and many of the legal rules in these areas are not harmonized. There is also a considerable lack of transparency as to the data protection practices of law enforcement and intelligence agencies throughout the EU.

Another EU directive (the ePrivacy Directive) provides additional rules for the electronic communications sector. There are also many Member State laws (including those in other areas, such as employment law) that are relevant to data protection.

Each Member State has at least one DPA, as does the EU for its institutions and bodies. The DPAs are the primary enforcers of data protection law in the EU. The CJEU sets high requirements for the independence of these authorities, meaning an absence of any external influence. The DPAs frequently publish opinions and papers dealing with data protection topics, both at the national level and jointly in the Article 29 Working Party.

The development of data protection law among the Member States has differed substantially, as does their awareness of data protection issues and their enforcement practices. Thus, some have a long tradition of data protection laws (including provisions in their national constitutions), while others came to the subject much later.

In 2009, due to the entry into force of the Treaty of Lisbon, EU law was changed to include stronger protection for privacy and data protection as fundamental rights. This included granting constitutional status to the EU Charter, which recognizes the right to data protection as a separate fundamental right next to the right to respect for private and family life. The Treaty of Lisbon also introduced a general legal basis for EU-wide rules on the protection of personal data.

In 2012 the European Commission proposed a reform of EU data protection law, including the replacement of the Data Protection Directive with a regulation. The adoption of a General Data Protection Regulation (GDPR) would increase legal harmony and consistency, since it would apply uniformly throughout the EU without the need for Member State implementation. The legislative process to enact the reform is underway, although it had not been concluded as of the finalization of this Report.

In general, compliance with and enforcement of EU data protection laws are inconsistent and insufficient, although they have improved in recent years. The amount of civil litigation for data protection claims has been limited thus far, though this may change when the proposed GDPR comes into force. Many public authorities have data protection officers (DPOs) to oversee their compliance with the law, and a growing number of private-sector entities have appointed DPOs as well. There are some certification schemes and trust marks in various Member States and in particular sectors, but none have become widely accepted on a pan-EU basis.

## B. PRIVACY PROTECTION IN THE US

Privacy protection in the US is based on concepts of autonomy and liberty articulated in the US Constitution and the Bill of Rights. The Supreme Court has held that the Constitution guarantees a right to privacy in many key respects, including an individual's right to be free from unreasonable government searches and seizures and to make decisions about matters of "fundamental" liberty (including abortion, contraception, marriage, procreation, private sexual conduct, child rearing, and education) without government interference. The Court has also identified a number of privacy interests implicit in the First Amendment, such as the rights of anonymous speech and private association, but the Court has at times identified privacy as a value in tension with the First Amendment's commitment to free speech.

US law also recognizes a "right to be let alone", based in part on the Fourth Amendment and the four "privacy torts": the public disclosure of private facts, intrusion upon seclusion, false light, and appropriation. But these torts have proven difficult to apply to data privacy.

The US also has enacted a number of important privacy statutes. In 1970, the US adopted the Fair Credit Reporting Act (FCRA). Then, in 1973, the Department of Health, Education and Welfare (HEW) recommended the adoption of a code of fair information practices for personal information held by the US government. The HEW Report has been highly influential in the development of privacy law, both in the US and abroad. For example, it was an important source of the 1980 OECD Guidelines, developed in parallel with the CoE's Convention 108 mentioned in II.A above.

The HEW Report provided the framework for other federal privacy statutes. The Privacy Act of 1974 requires the government to abide by the fair information practices in the collection and processing of personally identifiable information. The Freedom of Information Act provides a right of access to government-held information, but shields personal information from disclosure. Other federal privacy laws include the Children's Online Privacy Protection Act (COPPA); the Gramm-Leach-Bliley Act (GLB) (covering financial services); the Health Insurance Portability and Accountability Act (HIPAA); and many others. Taken together, these sector-specific statutes reflect the US's dominant harm-based approach to regulating privacy – i.e. enacting specific privacy statutes to govern the collection and use of information that, in Congress's view, is sensitive and warrants special protection.

Consumer protection agencies play an increasingly important role in policing data privacy and security in the private sector. Since the mid-1990s, the Federal Trade Commission (FTC) has relied on Section 5 of the FTC Act (which prohibits "unfair or deceptive practices" in interstate commerce), as well as

its authority under sector specific statutes such as the FCRA, COPPA, and GLB to regulate consumer privacy. The FTC engages in robust enforcement, and has thus far brought over 170 privacy cases, most within the past decade. The FTC's privacy orders generally run for 20 years, require the target company to establish a program to take privacy into account in all phases of a product's life-cycle, and to undergo third-party audits bi-annually to certify that it is complying with its privacy program. Where the company has violated an FTC rule or a prior FTC order, the agency may also impose civil penalties. The FTC also uses extensive collaborative, soft-power mechanisms to advance strong privacy practices and explore challenges in new technology areas. The agency holds workshops to bring stakeholders together and then issues detailed guidance on privacy issues. Other federal agencies, including the Federal Communications Commission, the Consumer Financial Protection Bureau, and the Department of Health and Human Services, are ramping up their privacy policy-setting and enforcement efforts.

States also play an important role in developing privacy policy and enforcing privacy norms in the United States. A number of states have constitutional privacy protections and many have enacted privacy legislation (such as security breach notification laws, and laws restricting voyeurism, paparazzi activity, un-consented to facial recognition, and misuse or abuse of drivers' license and voter registration data). California plays an especially important role: It has enacted strong consumer privacy laws and, due to its size and economic power, many large US companies follow California's laws nationally. Furthermore, every state has a deceptive trade practice statute that enables state Attorney Generals (AGs) to bring enforcement actions against companies for privacy-related violations. State AGs are also authorized to enforce several federal privacy statutes, including FCRA, COPPA, and HIPAA. Over the past ten years State AGs have played an important role in protecting privacy in the online marketplace, at times paralleling federal efforts, and at times breaking new ground.

Notwithstanding this welter of sector-specific laws, significant gaps in the US's privacy framework remain. To close these gaps, the White House in 2012 issued a report entitled Consumer Data Privacy in a Networked World, which called for a "consumer privacy bill of rights". At the same time, the FTC published a report entitled Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, urging Congress to enact broad, baseline privacy legislation that would establish that privacy is a basic right. In March 2015, the White House published a discussion draft of proposed legislation, but at present there is no proposed legislation based on this draft pending before Congress.

There are three other important sources of privacy protection in the US. First, individuals have a right to bring lawsuits in federal and state courts for violations of federal or state privacy statutes or the privacy torts. Private enforcement of privacy laws is becoming an important source of privacy protection, at least where the plaintiff can show economic harm. Second, industry has taken some important steps forward, including promoting Chief Privacy Officers (CPOs) within companies, creating privacy-enhancing technology, and, in some areas, developing binding codes of conduct that, if violated, can be the basis of enforcement actions by regulators. And third, many sophisticated non-governmental organizations (NGOs) push for increased privacy protection by, among other things, investigating and publicizing privacy issues; challenging the adequacy of self-regulatory models; bringing actions in court against the government and companies; leading broad-based coalitions seeking new privacy laws; and urging Congress to enact privacy legislation. The combination of advocacy work, engagement by CPOs, and media pressures for privacy-protection has pushed "privacy on the ground" in the US.

Recent developments have raised considerable concern about the adequacy of legal controls on the activities of US law enforcement and intelligence authorities. The Snowden revelations have shown that the national intelligence agencies have engaged in widespread data collection and analysis, without adequate accountability and transparency. These activities run counter to constitutional and

statutory protections against unwarranted surveillance and have spawned a vigorous debate in the US about the proper balance between privacy and security. Thus far the debate has resulted in the passage of the USA FREEDOM Act, which will end bulk collection of data under section 215 of the PATRIOT Act, as well as an evolving set of changes and various proposals from the Executive Branch and the Congress to reform national security surveillance laws and practices. These concerns are not unique to the US. Rather, similar concerns apply to law enforcement and intelligence activities in many other countries as well.

### C. COMMON SURVEILLANCE CHALLENGES

While the Privacy Bridges project focuses on commercial data privacy questions, we believe that certain basic principles with respect to national security surveillance are important to preserve trust in the global Internet environment. We therefore subscribe to three broad principles:

- All surveillance, including national security surveillance, must be conducted under the rule of law;
- Surveillance practices should be subject to reasonable transparency, proportionality, and accountability principles; and,
- All citizens should be accorded by other governments a basic set of rights, on a reciprocal basis.

It is well beyond our mandate, however, to offer any specific suggestions on how to implement these principles because that would require both changes in law and government-to-government negotiations on a bilateral or even multilateral basis, which are tasks that we leave to others.

# III. THE NEED FOR AND POSSIBILITY OF PRIVACY BRIDGES

## A. THE NEED FOR PRIVACY BRIDGES

As indicated below, the systems of privacy protection in the EU and the US share many common values. However, they also differ in some important ways, which illustrate the need for privacy bridges between them. The following are some of the main differences:

- The two sides have different conceptions of the principle of legitimacy as it applies to data processing. Under EU data protection law, a legal basis and a legitimate purpose are always needed before personal data may be processed. By contrast, in the US, generally speaking, commercial data may be processed unless there is some legal rule preventing it. (The US Privacy Act, however, requires certain conditions to be met before the government may process any personal data, and thus more closely aligns with EU data protection law.)
- The EU takes more of a precautionary approach to data protection than the US does. Such protection does not depend on the existence of any "risk or harm" because EU law recognizes data protection as a fundamental right.[4] The EU also places emphasis on the principle of proportionality. While the US Supreme Court applies a "reasonable expectation of privacy" standard in determining the validity of searches and seizures under the Fourth Amendment, analogous limitations in the consumer privacy context generally lack any constitutional basis. Instead, they arise from specific statutes, torts or FTC findings of unfairness or deception.
- The two sides tend to strike a different balance between privacy and freedom of expression. While there are important exceptions to this general rule, the US Supreme Court has at times tended to favor the First Amendment's protection for freedom of expression when it stands in tension with privacy, while in similar situations the CJEU has tended to favor data protection and privacy rights over freedom of expression.
- The two sides have different compliance cultures: The EU Directive establishes a high level of data protection but enforcement by DPAs so far remains limited (although the compliance approach among the EU Member States is by no means homogeneous). In contrast, the US has a myriad of privacy laws enforced by a variety of federal and state agencies, as well as the federal and state prosecutors and attorneys general. The FTC has emerged as a leading commercial privacy regulator and engages in numerous, fact-specific investigations of privacy violations that yield a "common law" of consumer privacy through enforcement actions, while Health and Human Services brings an even larger number of enforcement actions under HIPAA.

In recent years, the EU has strengthened data protection as a fundamental right in its constitutional structure; despite the strong role of the Supreme Court, one cannot envision similar constitutional changes as likely in the US. The US has seen both strong enforcement activity by the FTC and state AGs as well as broader adoption of technological protections for privacy, both of which are less well

[4] *The proposed GDPR does, however, include a consideration of risk in calibrating compliance with privacy principles and organizational accountability.*

developed in the EU. The US has also experienced an increase of privacy legislation and rulemaking at the state level, while the EU has been engaged in an effort to provide greater harmonization through the proposed data protection reform. All these developments have led many people on both sides of the Atlantic to view change in the other side's law as the only sound way to build common ground.

However, we do not believe that it is necessary to wait for legal reform or further harmonization to occur before starting to build bridges. Changing the law is an arduous and lengthy endeavor, and waiting for it to happen can become simply an excuse for inaction.

The common privacy threats that both legal systems face also highlight the need for practical bridges between them. For example, the Internet has made it possible for anyone to collect and process huge quantities of personal data, and it has become increasingly difficult to distinguish between the public and private spheres, particularly with regard to online data processing. The growth of data processing in non-democratic countries puts pressure on both the EU and US to better protect privacy, as does the increasing influence of global companies. And there is a growing trend for governments to access data collected by the private sector, and an inability to cope with the privacy risks this poses.

The need for privacy bridges also arises from the common shortcomings of the two systems. Neither the EU nor the US has been notably successful over the past few years in ensuring a consistently high level of privacy protection in practice especially in light of rapid technology developments. The EU system is widely seen as too focused on paper-based compliance and overly bureaucratic requirements, and the US system as too fragmented while lacking a consistent normative structure. There is also a woeful lack of understanding in both the EU and the US about each other's system of privacy protection.

Both sides also face the common challenge of ensuring that privacy rights are respected by their intelligence services. In both the EU and the US, the intelligence services seem to operate in a kind of parallel universe, where it is difficult to determine which legal standards are applicable to them, when they apply, and whether they are effective.

All of these factors strongly suggest that any opportunity to implement non-legal measures that produce interfaces between the two systems, in ways that protect privacy in practice, should be seized upon.

## B. THE POSSIBILITY OF PRIVACY BRIDGES

The possibility of privacy bridges derives from the common heritage of the EU and the US, the history of dialogue between them, and the common challenges they face.

Despite their differences, the EU and US are both liberal democracies with a high degree of respect for the rule of law. This provides common ground on which to build practical solutions for privacy protection.

There is a long history of cross-fertilization between the EU and US approaches to privacy. A few examples include the impact that leading US scholars (such as Alan Westin) and developments (such as the 1973 HEW Report) had on the early data protection laws in Europe; the appointment of CPOs and DPOs, which have become entrenched in both the US and the EU; and the passing of security breach notification laws, which were first enacted by the US states and were then adopted in the EU ePrivacy Directive and also in some EU Member States laws.

The social and technological realities in the EU and the US are also closer than the legal differences suggest. In both regions, there is widespread use of online technologies such as search engines and social networks and very extensive processing of the personal data of children, all of which raises

similar concerns on both sides of the Atlantic. These common concerns also raise the possibility of developing common technological standards for data collection and processing. In both regions, economic growth and development are largely dependent on technology and digital processes.

In addition, the globalization of data processing has created significant and shared challenges for both the EU and the US. The application of data protection and privacy law tends to be territorially based, but online services are largely indifferent to location, and use algorithms that assign data processing tasks based on processing times and available storage capacity rather than geography. Data flows increasingly occur not through point-to-point transfers, but by making data available globally through distributed computing services. There is no international consensus on the factors that should be used to determine what privacy law applies and how regulators can enforce national laws across borders. This leads to conflicts between different regulatory systems, overlapping legal obligations, and frustration among individuals. The EU and the US systems need to find ways to ensure that privacy rights are respected regardless of location.

Government officials and data protection regulators in the EU and the US also engage in a continuing dialogue concerning privacy. They both played instrumental roles in approval of the OECD Privacy Guidelines, including the original version dating from 1980 and the 2013 revisions. The US has been an observer in the data protection work of the Council of Europe, as has the Article 29 Working Party in the work of the Asia-Pacific Economic Cooperation (APEC) group (which includes the US). This demonstrates the ability of both sides to work together constructively in relation to privacy.

Practical privacy solutions can also help lead to better privacy law and regulation in the long term. Longstanding differences between the two systems are reflected in different institutional choices they have made, which cannot be quickly changed. The creation of practical privacy bridges can help build common practices and other commonalities between them over time, thus leading to better understanding beneath the regulatory level that can later provide the foundation for legal changes. There are many ways to affect behavior besides law (e.g. ethics, technology, regulatory cooperation, corporate responsibility, etc.), and it is at these levels that privacy bridges can work to bring the two sides closer together.

# IV. TEN PROPOSED PRIVACY BRIDGES

## A. INTRODUCTORY REMARKS

Over the course of four face-to-face meetings in Europe and the US, the Privacy Bridges group identified and debated a number of potential bridges. Relying upon the expertise of its members and their assessment of current privacy issues and policy shortcomings, the group eventually settled upon ten proposed privacy bridges. We believe that all ten bridges satisfy the three criteria identified above: privacy bridges must be practical, achievable without legal reform, and result in privacy improvements on both sides of the Atlantic. Bridge 1 proposes a more formalized mode of cooperation between the Article 29 Working Party and the FTC; Bridges 2-4 focus on enhancing user control over personal data as well as user redress; Bridges 5-8 suggest various ways for organizations to improve the privacy protection they provide to individual citizens and consumers; and Bridges 9-10 discuss longer terms initiatives for improving intergovernmental cooperation and coordinating privacy research agendas.

There is nothing magical about the number or content of these ten bridges. Certainly, other bridges exist or are waiting to be discovered, and we encourage anyone wishing to expand on our work to identify and publicize these new bridges in an appropriate forum.

## B. THE PRIVACY BRIDGES

We will now present and explain the ten proposed privacy bridges one by one in the order mentioned above.

### 1. FORMALIZING THE WORKING RELATIONSHIP BETWEEN THE ARTICLE 29 WORKING PARTY AND THE FEDERAL TRADE COMMISSION

Notwithstanding the marked differences in their legal regimes, regulators in the EU and US face the same challenges responding to the privacy issues posed by rapidly evolving technologies that capture and process personal data. In the EU, the principal entity that provides guidance on these cutting edge issues is the Article 29 Working Party, an organization composed of the DPAs from each EU member state as well as key EU privacy officials in the European Commission and the European Data Protection Supervisor (EDPS). In the US, the FTC, an independent agency of the federal government that has broad jurisdiction over commercial privacy issues, has a leading privacy policy voice based on its enforcement expertise along with other Executive Branch officials in the White House, the Department of Commerce, and other agencies with sector-specific privacy authority.

---

[5] *Our comments referring to the Article 29 Working Party apply analogously to its successor organization (i.e. the European Data Protection Board) under the proposed EU data protection reform.*

The Article 29 Working Party and the FTC should commit to regular, public dialogue and policy coordination on leading privacy challenges faced in the transatlantic region. There are already informal relationships between the Article 29 Working Party and FTC policy staff. This is not surprising. Both entities work on issues of common importance – ranging from the privacy implications of mobile applications to the impact that facial recognition and other biometric sensing devices will have on privacy to the privacy implications of the Internet of Things. And often, almost invariably, the policy advice given by the Article 29 Working Group and the FTC is consistent. But the exchanges between these entities have been ad hoc and episodic. As a result, the two entities are often working on the same issues at the same time without a channel to exchange ideas and proposed solutions before finalizing their work.[6]

One privacy bridge that should be built is to establish a formal foundation to institutionalize a cooperative working relationship between the Article 29 Working Party and the FTC. We propose that the two entities enter into a Memorandum of Understanding (MOU) that has several core elements, all of which will be designed to ensure cooperation on policy matters. Of course, each entity must remain free to reach whatever conclusions it believes are warranted under applicable EU and US law, respectively. But cooperation will inevitably yield better, and more consistent, policy formation and guidance on both sides of the Atlantic. We believe that such a framework for cooperation could be developed and adopted rather quickly, possibly even within one year. In any case, common work in developing this framework should start as soon as possible in 2016. This bridge should be developed in coordination with the Executive Branch bridge (Bridge 9), so that policy discussions amongst European Commission and United States Executive branch agencies are aligned as appropriate with the activities of the FTC and the EU Data Protection Authorities.

The benefits of strengthening the relationship between the Article 29 Working Party and the FTC are many. For one thing, collaboration will yield stronger, smarter, and more efficient policy development and enforcement, delivering enhanced privacy protection to individuals. It is time that the EU and US learned from one another; collaboration allows each entity to adopt the best practices available, so long as they are consistent with applicable law. Regulated parties will benefit as well. To the extent that collaboration encourages consistency in guidance across the Atlantic, regulated parties can avoid the costs of having to comply with divergent legal regimes.

To achieve the goal of meaningful cooperation, a number of steps should be laid out in the proposed MOU. First, the MOU would have to tackle the question of advance notification. The Article 29 Working Party and the FTC would have to put in place a system to apprise each party of undertakings by the other to explore a particular policy question. The FTC often precedes the issuance of policy guidance by holding one or more public workshops to get the views of companies, privacy advocates, and other regulators. These are information-gathering sessions that inform FTC's decision; the participants in these workshops do not play a role in the FTC's policy-making process. Notice to the Article 29 Working Party should be provided no later than the time the FTC decides to hold a workshop, so the Article 29 Working Party can participate if it so chooses. And ideally, an MOU would

---

[6] *Consider one example. The Article 29 Working Party and the FTC were simultaneously working on recommendations for mobile applications that collect and share data on children and teens. Although the two institutions did not collaborate – there was no information sharing or discussion of policy – their final recommendations were nonetheless quite similar. Compare FTC Press Release, FTC's Second Kids' App Report Finds Little Progress in Addressing Privacy Concerns Surrounding Mobile Applications for Children Kids' Data – Still Collected, Shared without Parents' Knowledge, Consent (Dec. 12, 2012), http://www.ftc.gov/news-events/press-releases/2012/12/ftcs-second-kids-app-report-finds-little-progress-addressing; with Article 29 Data Protection Working Party, 00461/13/EN, WP 202, Opinion 02/2013 on apps on smart devices (Feb. 27, 2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.*

encourage the entities to hold joint workshops, perhaps one in the EU and one in the US on a regular basis. For the Article 29 Working Party's part, the MOU should provide that it should notify the FTC when it begins to examine an important policy question.

Second, the MOU would have to include measures to ensure cooperation in policy development. To accomplish this goal, the MOU would have to lay out steps to prompt the parties to share information, research and preliminary ideas about policy guidance. The parties must commit to sharing information, discussing possible policy options, and exchanging drafts or at least holding conference calls to discuss tentative conclusions before any guidance document is finalized. As part of issuing any guidance, the parties also should inform one another of the guidance the party intends to provide so that, to the extent it is warranted and permissible under applicable law, the parties may seek to align their guidance.

Third, to the extent possible, the entities should acknowledge in their guidance the points of convergence between the findings of the Article 29 Working Party and the FTC. Each entity already acknowledges the other's work in their guidance documents. But more could be done. It would do a service for both entities (where possible) to make clear that on the most urgent new privacy issues, they have reached identical or similar conclusions about the appropriate measures that should be taken to protect privacy. In certain areas, it may even be possible to arrive at consensus standards, either immediately or in the course of time.

There are of course other measures that could be taken to strengthen the ties between the Article 29 Working Party and the FTC. For instance, the MOU could call for regular face-to-face meetings between the two entities, alternating between Brussels and Washington, D.C. The MOU could also encourage staff exchanges, which would permit FTC staff and staff of one or more DPAs or the EDPS to spend time learning how the other entity conducts its work. And the MOU could call for greater data sharing between the Article 29 Working Party and the FTC.

Finally, and distinct from cooperation on policy matters, the Article 29 Working Party and the FTC should work to develop a framework for more robust cooperation on enforcement matters involving trans-border violations of privacy law. After all, many of the enforcement issues that transcend national borders also raise important and often novel policy questions, and cooperation can conserve scarce enforcement resources. A Resolution on Enforcement Cooperation adopted during the 2014 International Conference of Data Protection and Privacy Commissioners (the Mauritius Resolution) recognized the reality that increased trans-border data flows affect large number of individuals across national borders and called on data protection authorities to forge bilateral and multilateral enforcement agreements. EU member states and the FTC have recently begun to enter into bilateral agreements that can provide the foundation for broader and deeper cooperation.[7] As these developments reflect, it is better for the data protection agencies to work collaboratively on these matters, rather than to proceed in isolation. At the EU side, these efforts could be coordinated in the Article 29 Working Party.

---

[7] *See, e.g., FTC Press Release, FTC Signs Memorandum of Understanding with Dutch Agency On Privacy Enforcement Cooperation (March 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/ftc-signs-memorandum-understanding-dutch-agency-privacy; FTC Press Release, FTC Signs Memorandum of Understanding with UK Privacy Enforcement Agency (March 6, 2014), http://www.ftc.gov/news-events/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency; FTC Press Release, FTC Signs Memorandum of Understanding with Irish Privacy Enforcement Agency (June 27, 2013), http://www.ftc.gov/news-events/press-releases/2013/06/ftc-signs-memorandum-understanding-irish-privacy-enforcement.*

## 2. USER CONTROLS

Users all over the world value the Internet and the World Wide Web. The applications and services that depend on them are important but sometimes complex. They raise real challenges to individuals' ability to exercise their rights to user control over personal data. They not only pose a barrier to individuals exercising their rights but also create confusion for businesses seeking to design their services in a way that respects individual choice and control. While legal regimes in the EU and US differ with regard to the nature of control and consent requirements, both have a common interest in easy-to-use mechanisms for expressing individual decisions regarding choice and consent. At the same time, service providers would benefit from having access to such mechanisms as well as a clear set of rules about how those mechanisms should be used.

This user control bridge calls for a collaborative effort on the part of privacy regulators, industry organizations, privacy scholars and civil society organizations, working together to make concrete progress on this challenge. 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. Both sides of the Atlantic have tried and failed to address this need. A user control bridge would do much to bring together the collective insight, authority and commitment of EU-US parties and do much to solve this problem.

As noted, the complexity of today's digital environment makes it difficult for users to know the identity or purpose of the organizations collecting personal data from them, how these organizations classify the data, when and why they use the data, who has access to the data, or whether they share the data with other parties, and so on. Additionally, these organization, especially those operating on a global basis, may find it difficult to meet the varying and sometimes conflicting legal obligations associated with offering certain services to users residing in different countries. A first step towards greater user control is more transparency, which we address in Bridge 3. However, transparency is only a secondary step, and remains incomplete unless users have the ability to control and make real choices about how organizations handle their personal data.

As explained in the previous chapters of this Report, there are differences in the laws of the EU and the US. For example, Article 6 of the Data Protection Directive provides six legal grounds for collecting and using personal data, one of which is consent. EU law further specifies that where consent is required, it must fulfill certain conditions: an individual should give his or her consent only as a "freely given, specific and informed indication" of his or her wishes. Consent should also be unambiguous and in some situations even explicit; inaction or silence is therefore not enough to establish valid consent. This does not necessarily preclude the use of other legal grounds for other types of processing operations, provided these operations comply with applicable law. Nor does it preclude explicit behavior that may amount to valid consent. In certain cases, where consent is not required, EU law may also give the right to object.

In the US, on the other hand, user consent is not universally required before collecting or using personal information, although sectoral laws and enforceable codes of conduct do usually contain a user choice requirement either on an opt-in or opt-out basis. However, sensitive data (such as medical or financial data) often carries an opt-in requirement, and some organizations may want to offer users choice mechanisms that are in between opt-in and opt-out. Thus, both the EU and US have an interest in making such choice mechanisms widely available.[8]

---

[8] *In this regard, questions about the market power of data collectors may be relevant to the dynamics of choice and consent. Both US and the European Union competition authorities address these questions.*

In order to design technical mechanisms that can be used across the Web to signal presence or absence of consent, as well as compliance with other legal requirements where relevant, it will be necessary for system designers and regulators to work together to establish clear guidance on how to comply with the relevant rules.

Tracking and collecting data on individual activity takes many different forms. However, we commonly distinguish between organizations depending on their underlying relationship with the user. Organizations interacting with individuals directly and visibly are the so-called "first parties". Other parties, such as advertiser networks and other firms that partner with the first party organization are usually referred to as "third parties", because they do not have a direct relationship with the individual user visiting a particular website. While first parties are of course subject to legal privacy requirements, contractual terms, and user expectations, users nonetheless have a direct relationship with them, and thus may generally have a reasonable expectation that first parties will collect certain types of personal information (albeit not with regard to all kinds of information, including (web) analytics and/or audience measurement). This has an influence on which legal requirements are applicable. But third parties are viewed very differently. While first and third parties may be subject to different legal rules and user expectations today, the user control mechanisms we develop should offer a consistent picture and user experience regardless of the nature of the collecting party. However, whether dealing with first parties or third parties collecting personal data, individuals should have easily understood and accessible mechanisms to express their privacy choices and have those choices respected.

Even if citizens of different countries have different rights based on their national law, all users have an interest in exercising meaningful control over the collection and use of their personal information. And all responsible data controllers will want to meet users' expectations regarding individual control. In fact, there has been a long history of trying to develop and deploy such user control mechanisms but the results have been mixed. We believe that a more successful effort is possible provided two conditions are met: (1) this new effort combines the energy of both EU and US participants, and (2) those designing the technology and business processes have clear guidance from regulators in both jurisdictions. The World Wide Web Consortium's Tracking Protection Working Group, for example, has already undertaken technical design and standardization work necessary to facilitate informed choice enabling users to signal their intentions and preferences. There is an opportunity now to build on this work in order to meet the increasingly urgent need for user control techniques in a variety of new application areas.

To ensure that individuals remain in control of their personal data and enjoy a high level of protection, users should be able to express their preferences irrespective of who handles their data. In other words, users should have a simple tool to express their preferences with regard to the collection and use of their personal data, especially when third parties are involved, in accordance with the applicable law. This approach benefits users by enabling them to express their wishes regarding the collection, use, and sharing of their personal data, while ensuring that all organizations – including both first and third parties – respect these wishes in subsequent uses or transfers. It also benefits organizations by ensuring that they can offer services internationally while complying with regulations in multiple jurisdictions.

In order to build this user control bridge, we recommend that representatives from the research and industry sectors work together to design, implement and test technical solutions that both enhance the compliance of organizations operating on different continents and provide users more control over their personal data. The main requirements of such a system are:

- *Easy-to-access information about what data is collected, by whom, and for what purpose.* The user control mechanisms must be integrated with a widely used set of tools that give easy access to information about privacy practices. We do not recommend a universal or comprehensive effort to cover all

details of privacy policies, as this complexity would overwhelm users. Rather, there should be guidance from regulators and engagement with industry and civil society groups to determine what aspects of data handling are most important.

- *Easy-to-use expression of individual choice with respect to data collection and use.* This will require that, depending on the legal framework applicable and following the privacy by design principle, the default settings ensure compliance with the applicable rules. Where the basis for collecting as well as data use (partly) depends on the user's preferences, these preferences must be expressible in a manner that is easy and persistent, both in time and across devices. Furthermore, these mechanisms should be applicable across a wide range of technologies, not limited merely to the data collection technique of the moment (such as cookies).
- *Clarity about implementation and legal requirements for commercial implementers.* Those commercial entities using the new user control mechanisms should have a clear indication that if they deploy these new systems in good faith, they will benefit from clear guidance concerning compliance with legal rules on both sides of the Atlantic. This will be necessary to assure that technologies are designed correctly and that business has an incentive to deploy the new systems.

In sum, more than just technical standards are required to make such a system work. All parties require concrete guidance about the applicable legal requirements in various policy contexts. EU and US regulators can help speed the adoption of such user control systems by developing clear scenarios showing how the aforementioned technical solution would apply in different situations. Every legal eventuality needs not be specified. Rather, if all parties understand the legal requirements in popular usage scenarios, the system is much more likely to be adopted and available to users around the world.

## 3. NEW APPROACHES TO TRANSPARENCY

Many individuals have voiced concerns that they are not in control of their personal data. This is partly due to companies and governments not being sufficiently transparent about their collection and subsequent use of personal data and partly to the speed of technological development. As noted above, individuals are frequently not aware of the choices they have or how to exercise those choices (e.g. to opt-in or opt-out of data processing). Nor are they aware of their rights with respect to their personal data (e.g. the right of access, correction, and objection). The result of this lack of transparency is a rising distrust of digital service operators.

We recommend a more user-friendly form of transparency as a necessary condition of the user controls described in Bridge 2. The two key elements of user-friendly transparency are: (1) meaningful notice to individuals for the collection and use of personal data by companies and public organizations whether or not they have a direct relationship with the consumer or citizen, and (2) access for individuals to their personal data held by companies and by public organizations.

For these elements to be addressed in a user-friendly way, standardization on both sides of the Atlantic will be critical. Companies and public organizations must provide notices and responses to data access requests in a meaningful, accurate, easily accessible, comprehensive and useful format. We recommend that the FTC and Article 29 Working Party cooperatively elaborate guidelines for the essential elements of standardized notices and access reports.

At the point of collection people should be enabled to make rational choices on whether to share data with a service. This means that they need information on the collection, use, aggregation, and other data processing activities, automated decision making, sharing, and secondary use practices (including information on types of data recipients), as well as data retention and security practices.

Layered policies have been put forth as an important way forward for notifying people, but they still may be too complex as we move into ever more ubiquitous computing environments. They are also not standardized for machine-readability. Simple, machine readable and standardized means such as symbols, signs or ranking tools need to be developed, used and tested on both sides of the Atlantic to ensure transparency for individuals.

Ongoing work developing standardized notices by major companies, universities and political bodies already exists (for example, efforts by the Mozilla Foundation, the University of Ulm, and the European Parliament, as well as the Carnegie Mellon-Fordham-Stanford Usable Privacy Project). These efforts focus on innovative solutions to display privacy policy information to individuals from the perspective of individuals and to integrate more transparency in the technology. While these efforts are very important, they are challenged by a lack of consensus on the critical elements that make notice meaningful and they may result in multiple inconsistent standards that risk additional confusion for individuals.

To avoid this problem, the Article 29 Working Party and the FTC (who have already worked extensively on user notices) should pool the insights that they gained from these earlier and ongoing standardization efforts. Additionally, they should research the lessons learned in other industries on required notifications (e.g. nutrition labeling or consumer information in the retail industry) and apply them in the privacy context.

Based on these shared insights, the two entities should clarify at least the following four essential elements of notice:

- What information is really needed for consumers and in what contexts, e.g. information about all uses of data or only about perceived unexpected uses? At present, there are differences in the type and form of information about data processing activities that consumers receive. Notices, whether by text, signs, symbols or other means, must be meaningful for users in context and must be useful in the sense that users can act upon them.
- Who is responsible for notice? When data collection and processing are distributed, it is often unclear who is responsible for informing the user. For example, when social network data is re-used by insurance companies to reduce fraud, then consumers should have a means to know about this. But should the social network inform its users that their data is re-used for such purposes, or should the insurance company? Or both?
- What quality thresholds must notices meet? For example, the level of accessibility (e.g. machine-readability, visibility, device-independence), accuracy (i.e. truthfulness, completeness, timeliness) and level of comprehension (e.g. ease of understanding) are critical.
- What rules are needed to assure that notices accurately represent an organization's actual practices?

We envision the FTC and Article 29 Working Party relying on the MOU described in Bridge 1 to coordinate their recommendations on notices and then jointly encourage standardization efforts.

Transparency also requires that individuals have access to the data organizations hold about them and information on automated decision-making that is based on their data. Access to this information must meet several requirements. Access reports must be meaningful. When European users request access to their data today they often receive gigabytes of unstructured data. Sometimes they receive everything a company holds about them. Meaningful information requires that when companies share data with users they rely on standardized means of disclosure and that access reports should display the information in a comprehensible form.

Similarly, access reports must be accurate and complete. This means that users must receive the data relating to them as well as information about the sources and uses of data, including the identification of recipients of the users' data and inferences made about the user from the data. Finally, access reports need to be readily accessible. This implies that privacy information should be obtainable in common locations where data subjects expect to find them, and increasingly in automated form.

## 4. USER-COMPLAINT MECHANISMS: REDRESS FOR PRIVACY VIOLATIONS BY SERVICES OUTSIDE A USER'S OWN REGION

Individuals have a substantial interest in ensuring that personal data about them are used consistent both with applicable laws and with any commitments made when the data were first collected or used. In an environment of global data flows and Internet-enabled commerce, individuals often face a particular burden seeking help for possible privacy violations that occur outside of their own country or region. It may be hard for them to identify the applicable jurisdiction and the competent legal authorities. Individuals may not know of or understand their rights under the legal systems of other countries. And individuals may not be able to communicate with the relevant company or competent government authority in his or her own language.

In addition, different nations have varying laws as to which authorities can receive complaints and how those complaints should be handled. For example, within the EU, while all countries are required to have DPAs, some countries have a legal requirement that the DPA must start an investigation after receiving a complaint, while in other countries, the DPA has discretion as to whether or not to investigate complaints. In the US, complaints regarding alleged privacy violations may be brought to the FTC, state AGs, or appropriate sectoral regulators, but they typically do not investigate individual complaints, unless specifically required to do so (e.g. under the US-EU Safe Harbor Agreement).

Many complaints concern both data protection and consumer protection, especially in the case of Internet services. In the US, the FTC and other authorities are competent for both areas whereas in most EU member states, the DPAs are not enforcing consumer rights, which have been set out in the EU Directive on Consumer Rights 2011/83/EC. Therefore, we see the need to intensify the information exchange and cooperation between the relevant stakeholders in both fields.

Given how many of the challenges facing cross-border dispute handling are the result of differences in laws or issues intrinsic to international commerce, we are unlikely to solve any of them here. However, there are practical bridges that could help diminish their impact on individuals, increase the opportunities for individuals to ensure that they receive the full benefit of the applicable law wherever their data are located, and reduce the burdens they face when doing so. We recommend the following:

- As discussed above, individuals rely on transparency to inform them of how organizations collect and use personal data and to exercise their rights. We therefore encourage data controllers, whether or not required by law to do so, to make readily available on a website (or by other readily discernable means) information about the entity's identity and how the entity may be contacted concerning data protection issues. Where possible, this information should be provided in the major languages of the people whose data are likely to be collected or used.
- We encourage the EU Commission and the Department of Commerce 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, including data protection authorities, law enforcement agencies, state or provincial authorities, courts, operators of privacy seal programs, and private sector consumer protection and dispute resolution organizations. To the extent appropriate, this information should be made available to the public online and through other accessible means, and

in the major languages of the jurisdictions included. These efforts could build on the model of the FTC's Sentinel network and the European E-Justice Portal.

- The Article 29 Working Party, national European DPAs and the FTC should codify how to deal with cross-border complaints and implementing frameworks, consistent with existing law for referring complaints brought in one country to the government authority appropriate to review the complaint. And, as noted in Bridge 1 above, the Article 29 Working Party and the FTC should establish additional means to cooperate in the investigation of complaints building on existing platforms.

****

We turn now from bridges enhancing user control over personal data and user redress to those that would improve the manner in which organizations protect the privacy of citizens and consumers.

## 5. GOVERNMENT ACCESS TO PRIVATE SECTOR PERSONAL DATA

As noted previously, digital technology permeates all aspects of our lives. In particular, telecommunication and Internet service providers collect huge amounts of data in the context of their businesses. One point of the modern information society we have yet to fully emphasize is its globalized nature, with data crossing borders and continents at the touch of a fingertip. Cloud services further decouple data storage and processing from a specific location or territory. Not surprisingly, governments are highly interested in all this data communicated and stored globally. Most countries require providers of electronic services to hand over metadata and content data to law enforcement authorities and intelligence services subject to various legal conditions and procedures.

Government access to personal data held by private firms touches upon individual rights and freedoms granted by the UN Charter of Human Rights, the European Charter of Fundamental Rights, other transnational legal instruments, and national constitutions.

The legal requirements for government access are a matter of domestic law and they vary from country to country. National legal systems focus on the protection of their own citizens and of persons living permanently in their countries. Thus, the level of protection for data related to individuals outside their own country is often lower than for nationals.

As a result, privacy protections are highly fragmented and there is deep uncertainty and conflict for both individuals and the private sector firms holding personal communications and metadata as to the level of protection available in any given case. Moreover, these firms find themselves in the uncomfortable position of a piñata. While they are not in the surveillance business, they have become a key supplier of the architecture and the data that fuels government surveillance globally. They are on the front lines of privacy battles facing increasingly vociferous and competing demands of assistance from law enforcement and national security organizations, on the one side, and data protection and privacy regulators, civil society, and users, on the other.

From the perspective of human and civil rights, government access to data has to meet basic principles: Rule of law, proportionality, oversight, and redress, even where access concerns data of foreign persons.

Surely we must reform our laws, legal institutions, and governance choices to address the growing privacy issues of government access, especially as to access requests referring to data concerning cross-border data processing - but calls for specific legal reforms are beyond the mandate of our project. However, in the shadow of international human rights norms and commitments, which speak to both the public and private sector, we see as well the emergence of bottom-up responses to the global nature of surveillance. The nature of the problem, and these nascent responses, provide fertile ground

for building bridges. We therefore offer four recommendations for addressing government access to private sector personal data:

- Companies should establish common corporate practices for dealing with surveillance requests regardless of jurisdiction, citizenship, and location of data. This will advance the interests of privacy, provide more predictability, and ideally set a strong baseline of privacy-sensitive policies to inform legal reform, if and when it emerges.
- Companies should consider incorporating standards and best practices for handling government requests for personal data under the umbrella of Corporate Social Responsibility (CSR). Doing so helps socialize best practices, such as those developed by the Global Network Initiative (GNI), and has several other benefits. It would leverage the ability of corporate stakeholders to act as a check on government surveillance, provide a framework for assessing and responding to requests concerning data outside national territory, and create a process for dealing with legal conflicts arising due to different legal systems. (See Annex IV for the relevant portions of the GNI Implementation Guidelines.)
- Organizations that are competent for the oversight of government data access in the US and in Europe should exchange information and where appropriate cooperate in carrying out their tasks. They should develop proposals for improving legal oversight and protecting human rights in government surveillance activities both within and outside their territory and regardless of citizenship.
- Governments should be as transparent as possible about rules and practices of data access. They should inform the public about the frequency and nature of surveillance and data access orders. They should assess the effectiveness and efficiency of surveillance and access to data and they should publish the results of the assessment. Governments should also allow companies to report on government access to their data.
- Consistent with any legal reforms allowing company reporting, companies should report on practices relating to government access requests on a regular basis (at least once a year). Reports should specify the requesting authorities, the nature and the legal basis of access requests, quantities of requests, type of customers affected, and released data. They also should make public, to the extent possible, how far they have legally challenged access requests.

## 6. DE-IDENTIFICATION OF PERSONAL DATA

The availability and use of large data sets for research purposes directly benefits society. It enables scientific breakthroughs, commercial innovation, and improvements in government services including health, education, transportation, housing, and public safety. While there is no denying the social utility of data analysis and research, those who provide their own personal data expect a high level of protection against a variety of privacy harms, ranging from inconvenience or embarrassment to identity theft.

One of the most common tools for protecting the privacy of data subjects is de-identification, which is the process of manipulating or transforming a data set to make it very difficult to discover a person's identity or attributes. With the collection of very large data sets and the improvement of analytical techniques (the so-called age of big data), the successful de-identification of data subjects has become a very difficult challenge. This challenge – which also may be described in terms of preventing reidentification – will only become harder with the growth of networked objects (the Internet of Things).

De-identification techniques, therefore, are the subject of intense research and debate. The main techniques, namely randomization and generalization, include noise addition, permutation, aggregation, and various quantitative approaches to generalization such as k-anonymity, l-diversity and t-closeness. All of them have strengths and weaknesses and there are many examples in

the literature of common mistakes and failures related to their use. Many question whether de-identification is still possible today given a number of highly publicized re-identification attacks. A newly developed set of techniques called differential privacy seeks to prevent the leakage of a data subject's personal information by allowing researchers to submit statistical queries to a data custodian without the need for any direct access to the underlying data sets.

All of these techniques involve some tradeoff between privacy and data utility. Moreover, the current state of the art of deidentification is such that it is not possible to specify in advance a set of generic requirements that would apply for any and every data set or research scenario. For regulators, this means that a "one size fits all" approach is unavailable. Rather, regulators must consider minimum recommended parameters on more of a case-by-case and sector-by-sector basis.

Despite the difficulty and complexity of the techniques under discussion, it is important to note that de-identification has multiple regulatory consequences. First, it helps satisfy legal obligations such as data minimization and observing limits on data retention; second, it reduces the threat of harm in case of a data breach; and, third, it reassures data subjects that organizations engaged in data analysis will respect their privacy expectations. This last point is critical. Research projects involving data analysis or large data sets inevitably raise doubts about the reliability of deidentification and a more general public anxiety over the safety of any personal data collected into large data sets. Deployment of reliable deidentification techniques is essential to restore this trust. We believe that a joint EU-US approach would significantly improve the trust rebuilding process.

Fortunately, regulators on both sides of the Atlantic already share very similar views about the appropriate methods for deidentifying data. These "best practices" include a mix of regulatory, technical, and organizational measures. Although these methods are premised on distinct legal definitions of personal data, this is not a serious obstacle to constructing privacy bridges because best practices consist less in formal legal requirements than in a shared understanding of what constitutes reasonable means of deidentification. Indeed, discussions of deidentification methods are mostly found in informal policy instruments, such as reports[9], opinions[10], and codes of practice[11], rather than informal legislative enactments[12].

For present purposes, we may briefly consider three key aspects of sound de-identification practices that provide the basis of regulatory convergence:

- A risk-based approach in which organizations assess the risks associated with de-identifying data in light of the current state of de-identification techniques and re-identification methods and the availability of public data sets that might assist in re-identification; perform ongoing assessments as appropriate; and document these and other steps to permit regulatory oversight.

---

[9] *Federal Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers (Mar. 2012).*

[10] *Article 29 Data Protection Working Party, 0829/14/EN, WP 216, Opinion 05/2015 on Anonymisation Techniques (Apr. 10, 2014).*

[11] *United Kingdom, Information Commissioner's Office, Anonymisation: Managing Data Protection Risk, Code of Practice (2014) http://www.ico.gov.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx.*

[12] *The most notable exception is HIPAA. The HIPAA Privacy Rule provides that individually identifiable health information is deidentified by the removal of eighteen specific identifiers. See 45 C.F.R. § 164.514(b)(2)(i) (2010).*

- Use of rigorous de-identification techniques such as removal of direct and indirect identifiers; suppression of unique or unusual attributes; randomization via noise addition, permutation, and other techniques; and various forms of generalization. These techniques should be supplemented where appropriate by the use of query-based techniques (such as differential privacy) in which researchers interact with data by posing questions but never obtain direct access to the data sets.
- Protecting de-identified data by supplementing technical measures with organizational measures including internal policies and security firewalls limiting internal access to de-identified data, and data use agreements imposing strict limits on the data's use and disclosure by third parties, including terms prohibiting the re-identification of data received subject to the terms of a data use agreement.

Building on the existing convergence in best practices for de-identification, EU and US regulators might take several additional steps to ensure even better harmonization. For example, they might consider inviting a group of technical and legal experts to attend a joint workshop and then issue joint recommendations on the requirements of a risk-based approach, the strengths and weaknesses of specific de-identification techniques, and/or the appropriate organizational measures in support of de-identification.

Alternatively, the two sides might co-sponsor an IETF or W3C process for defining de-identification techniques within a risk-based framework and commit to incorporating any resulting standards into their distinctive regulatory systems. Domain-specific standards may also be developed allowing for more precise results in a given domain such as health research, genetics, social network research, or transportation planning.

Ideally, agreement on joint recommendations would enhance legal certainty for both EU and US organizations that follow these recommendations (i.e. a presumption of compliance with applicable legal obligations under EU and US privacy law, respectively). Regulators might also agree to develop model clauses for data use agreements as well as model language for civil or criminal statutes prohibiting the re-identification and/or disclosure of de-identified personal information, subject to a robust exception for white hat security research. At an even more ambitious level, both sides might encourage regulated organizations, advocacy groups, and individual users in the EU and US to share their knowledge and expertise and support the development of enforceable codes of conduct regarding de-identification.

## 7. BEST PRACTICES FOR SECURITY BREACH NOTIFICATION

A foundational element of privacy is securing personal information and thereby protecting it from unauthorized access, misuse, or abuse. In the US, there are a few states (such as Massachusetts) that encourage standards for establishing corporate "information security programs", and there are some EU member states (such as Germany and Spain) that identify certain levels of security measures and encryption that companies should use to protect personal information. Otherwise, security standards for personal information are often described as "appropriate", "reasonable", "commercially reasonable", or "industry standard". Regardless of what security standards exist, there will be breaches of personal information. There is inconsistency about whom to notify in case of a data breach and for what purpose.

In the US, even when there are no laws establishing security standards for the protection of personal information, most states (47 out of 50) have passed laws that require the notification of affected individuals if their personal information has been breached or subject to unauthorized access. California passed the first state data breach notification law in 2002, starting a domino effect that has led to region-specific data breach laws across the US. There is some evidence that breach notification laws increase firm incentives to invest in security to avoid reputational sanctions and loss of customers trust.

The hallmark of all US data breach laws is that they are data element specific. For example, HIPAA and its update, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enumerate what data elements are considered protected health information and establish a federal breach notification requirement for such information. The Family Education Rights and Privacy Act (FERPA) creates disclosure limitations on student education records. Additional federal laws exist that protect the privacy and disclosure of data in other sectors such as finance and telecommunications. The elements that trigger breach requirements are generally "sensitive" data elements that could cause harm if disclosed or misused; generally, personal data alone (e.g. a name) do not trigger data breach notification requirements.

The FTC can investigate and bring enforcement actions against companies with deficient security measures, pursuant to its unfair and deceptive trade practices authority. The Federal Communications Commission also has the authority to bring investigations and enforcement actions against telecommunications providers for poor security measures. Collectively, these laws and the threat of enforcement provide some basic security incident response parameters, but there are differing reporting triggers within each statute, creating a complicated compliance regime even though the intent – notify users so they can protect themselves – is relatively simple.

Except for specific data breach notification duties imposed on telecom operators and Internet access providers by the ePrivacy Directive, the EU does not yet impose a generic data breach notification law. As to personal data processing, although the Data Protection Directive 95/46 does not explicitly require data controllers to notify data breaches, it is more or less commonly accepted that the present technical and security obligations incumbent on data controllers indirectly encompass a notification duty.

New legislative developments are rapidly changing the EU regulatory landscape: data breach notification requirements have recently been or are being introduced for trust service providers (Trust Services Regulation), information society service providers and critical infrastructure operators (Draft NIS Directive), and data processor and data controllers (Draft GDPR).

The basic principles of the notification duties in all these statutes are roughly similar and generally include at least five elements: the scope of the notification duty, the time frame of the notification, the recipients of the notification, exceptions to notification, and the contents of notification. (For more details regarding each element, see Annex V.)

The need for good data security is crucial for privacy, and having some mechanism to address deficiencies including notifying affected individuals is an important principle. However, as preventative measures, organizations should create and support an information security corporate program and governance that will help avert security breaches or minimize their impact if they occur.

Information governance provides a framework in which organizations can catalog and control their personal information, including rapidly identifying security breaches when they occur. Mature organizations have implemented information governance as a pro-active measure to avoid security incidents (see also Bridge 8 on Accountability). Ironically, the public attention on data breaches has empowered many Chief Privacy Officers and Chief Information Security Officers, resulting in more staff and visibility after security incidents occur. Nonetheless, having a robust information governance system (incorporating all aspects of privacy, data protection, information security and information technology) will help ameliorate the risk of security breaches. While security breaches are nearly impossible to avoid, having a system in place should minimize the impact.

An aspect of organizational information governance is to help identify and categorize risk factors, in order to assess the security breach when it occurs. Additional work by policy makers and

by multinational organizations on what risk means and how to measure it would assist in the development of more international standards on evaluating risks associated with security incidents.

The data breach notification laws may be both under regulated (limited to specific types of provider in the EU) and over regulated (limited to certain data elements in the US). Furthermore, it is unclear what notification accomplishes in several situations – for example when individuals cannot take any action to protect themselves, or if there is no evidence of harm. Also, proposed time frames for notification, particularly in the EU, are unrealistic and set up a scenario where the notification will inevitably be inaccurate due to the speed with which the notification must occur. Researching and investigating breaches can take days or weeks; therefore whatever conclusions have been reached initially may not be accurate and certainly will not be complete.

In short, information security breaches have a global impact. They are cross-border by nature, not triggered or limited by local laws. The response should also be global. However, a lack of international cooperation between relevant authorities when dealing with breaches and a lack of internationally harmonized and legally accepted breach reporting methodologies may decrease the level of privacy protection of the end-user. There may be legislative efforts to increase the burdens and pressures on affected companies in order to appear "more privacy centric" without having the concomitant impact on end users. The obvious solution is a more harmonized approach to security breach notification. Greater consistency would surely benefit both companies and consumers. Once policy makers decide to impose notification duties, they should ensure the technical and practical details are aligned with each other. Technical and organizational requirements are capable of being linked together with standardization efforts, which should take place on an international basis, rather than a regional or national basis. Organizations should create and support an information governance regime that will help prevent security breaches or minimize their impact if they occur. It is also important for companies to follow international, cross-border best practices as security breaches often occur across jurisdictional boundaries. Finally, the legal threshold standard (risk-based, strict liability, negligence) should be consistently applied. If it is risk-based, the risk factors need to be considered and standardized.

We recommend the following measures for building trans-Atlantic bridges relating to security breach response and notification:

- Enforcement agencies on both sides of the Atlantic should cooperate in dealing with security breaches.
- Security breach standardization efforts (including the scope and detail of regulatory and consumer notification) should be organized at international level and not at a national or regional level. Multinational organizations should participate, and share experiences.
- Policy makers should work to harmonize their laws and policies in responding to data breaches, including identifying consistent risk factors, providing realistic response times, and specifying actionable steps for affected individuals.
- Organizations should create and align best practices and protocols to identify and report on breaches internally.
- Organizations should create and support an information governance regime that will help prevent security breaches or minimize their impact if they occur.

## 8. ACCOUNTABILITY

Organizational responsibility for data practices (or what many commonly refer to as "accountability") forms a critical part of effective data protection. Accountability can play a role in responsible information and privacy management practices by offering higher assurances of data protection to individuals and data protection authorities alike.

Accountability requires an organization's commitment to and implementation of strong, legitimate and fair information and privacy management practices; an organization's ability to demonstrate the existence and effectiveness of these practices to individuals, regulators, the public, and business partners and internally to management and corporate boards; and an organization's commitment to mitigation and redress for information and privacy management failures. Accountability encompasses not only best practices related to government requests for data, proper de-identification of personal data, and security breach notification procedures, but also much more. It is both broader and deeper than any single set of best practices.

In the past few years, regulators in a number of jurisdictions have accepted the idea of organizational responsibility as a means to assure data protection and satisfy local obligations. For example, the EU permits the use of Binding Corporate Rules (BCRs) to satisfy the adequacy test for data transfers under the Data Protection Directive. BCRs, which must be approved by the local DPA, require an underlying privacy program and compliance infrastructure, impose binding privacy obligations on the organization and its employees and have redress mechanisms for the individual whose data is being transferred. In the Asia-Pacific region, the APEC Cross Border Privacy Rules (CBPR) provide another example of an accountability mechanism, certified by an independent third party.[13]

Data privacy authorities in Europe, North America, South America, and Asia, have also issued guidance for their expectations of accountability mechanism and corporate privacy management programs.[14] The French CNIL has taken a further step by recently announcing an accountability seal, which it awards to organizations for privacy programs that satisfy French law and reflect accountability requirements. Similarly, in the US, FTC enforcement actions often require firms to adopt comprehensive privacy programs as part of a binding consent decree. In short, corporate privacy programs have become an integral part of corporate compliance efforts in many settings and regions. All of these accountability mechanisms have four factors in common:

- Substantive privacy rules that are binding on organizations;
- Institutional measure to ensure compliance with the rules;
- Some form of external verification or certification; and,
- Redress for violations of the substantive privacy rules.

Thus, organizational responsibility is an obvious bridge for addressing differences between the EU and US privacy systems. This bridge offers individuals an improvement in actual data processing practices, corporate responsibility and trans-border enforcement. And it offers companies effective compliance for international operations. Regulators have already reached some consensus on the promise of accountability mechanisms and have accepted certain prerequisite legal frameworks along with providing regulatory guidance. On the company side, those organizations that make commitments to accountability programs signal a willingness to apply a uniform standard of privacy protection to all of its business units on a worldwide basis. This may result in a positive dynamic whereby some

---

[13] *The Article 29 Working Party and the APEC Data Privacy Subgroup have already undertaken steps to develop tools to make it easier for companies that seek approval under both the BCR and CBPR. To date, a joint working group has created a mapping document called the Common Referential for the Structure of the EU System of Binding Corporate Rules and APEC Cross Border Privacy Rules System, which identifies both commonalities and gaps between the two sets of rules. Ongoing work focuses on allowing companies certified or approved under one system to benefit under the other system as well.*

[14] *Some examples include the Canadian Privacy Commissioner's 2012 Privacy Management Framework, https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf; the Hong Kong Privacy Commissioner's Privacy Management Programme, https://www.pcpd.org.hk/pmp/; and the Article 29 Working Party Opinion 3/2010 on the Principle of Accountability, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.*

companies agree to abide by one set of privacy (and security) rules that exceed the legal requirements in many of the countries where they do business. In some countries, accountability may ensure practical privacy protections for individuals that may be stronger than exclusive reliance on local law. Lastly, for data privacy authorities, accountability programs are co-regulatory mechanisms that can help facilitate corporate compliance, especially with respect to rapidly emerging technologies and new uses of information, thereby ensuring that privacy principles remain technology neutral and persist over time.

To be an effective bridge, organizational responsibility needs to encompass a set of common elements for corporate accountability programs. Many of these elements are already found in FTC consent orders related to data privacy, in the EU's BCR requirements, in privacy regulators' published guidance, and in some existing privacy laws. The common elements are:

(a) privacy requirements that contain substantive privacy and security rules setting out meaningful data protection consistent with applicable laws, regulations, standards and industry codes of conduct, which are uniform and binding on all corporate units across the entire spectrum of business operations and services;
(b) oversight by top management;
(c) privacy professionals to assure proper internal corporate implementation;
(d) risk assessment at various levels (programs, product, services, and technology), which includes assessment of both organizational and individual risks;
(e) policies and procedures to implement the privacy requirements including instructions about the collection and processing of data;
(f) training and awareness that ensures that employees understand program requirements and related policies/ procedures;
(g) verification that consists of internal and external audits and assessments to verify and certify effective implementation;
(h) response mechanisms that provide means for individuals to complain about privacy violations, means for breach notification and means for organizations to address any discovered deficiencies through internal enforcement; and
(i) redress for violations of the privacy requirements.

For organizational responsibility through accountability mechanisms to create a sustainable and long-term privacy bridge, we make several recommendations on how accountability might be supported:

- The FTC and the Article 29 Working Party should through public proceedings develop a set of common expectations for the elements of accountability programs. This would help industry demonstrate legal compliance and promote effective protection for individuals.
- Organizations should continue to provide for the development of privacy professionals. Chief Privacy Officers and other qualified professionals must be trained, certified and recruited by organizations, and provided with adequate resources and authority to discharge their role and responsibilities.
- The private sector should develop effective means for external verification. Meaningful verification will require (a) the development of information accounting and audit standards; (b) education and training for auditors; (c) accreditation of third-party certification organizations; and (d) certification of auditors verification mechanisms, which should be mutually recognizable to the extent possible.
- For small and medium enterprises (SMEs) engaged in cross-border activities, the private sector should focus on scaling accountability programs so that they may also enable SMEs to demonstrate their organizational responsibility. This is critical because SMEs will be an ever-growing part of the digital ecosystem in data driven economy.

- In working towards greater convergence of accountability measures, industry must propose and adhere to strong substantive privacy requirements that satisfy existing standards (such as BCR and CBPR)[15].

****

Finally, we turn from bridges improving organizational privacy practices to those addressing intergovernmental cooperation and collaboration on privacy research.

## 9. GREATER GOVERNMENT-TO-GOVERNMENT ENGAGEMENT

Government agencies in the EU (including both at the EU level and in the Member states) and the US (under the executive branch) play an important role in privacy policy making along with the leading regulatory and enforcement authorities. Government departments will address societal, technological, scientific, and commercial developments in a number of sectors of the transatlantic economy such as new transportation systems, drones, and medical research, all of which pose privacy challenges. As a bridge between these parallel government efforts, we propose active dialogue and, where appropriate, effective coordination between European and US executive agencies and decision-making bodies.

This privacy bridge is especially important in light of the different statutory and institutional privacy structures in the US and EU. The decentralized US approach disperses the implementation of existing statutes, regulations, policies, as well as the consideration of the need for new privacy laws, across a number of Cabinet agencies, under the ultimate direction of the White House. In the US, a variety of cabinet agencies face new privacy policy development and implementation questions. For example, the Federal Aviation Administration is developing general regulations for drones (unmanned aerial vehicles) and the US National Telecommunications and Information Administration is working on privacy codes of conduct regarding drone usage. Furthermore, many other federal agencies will use drones and are likely to collect personal data. The Department of Health and Human Services is examining rules and procedures for use of personal data in health care research. In some cases, existing statutory authority covers these uses of personal data, but agencies face implementation questions. In other cases, new technologies pose questions about how to apply privacy principles to both government and private sector activities. These questions are necessarily considered in the context of a range of policy priorities.

---

[15] *The Article 29 Working Party recently endorsed three measures discussed with the APEC Data Privacy Subgroup to assist organizations in implementing requirements from both the BCR and CBPR systems. The three measures are as follows:*

*On a short/mid-term basis, develop:*

1) *A common application form based on the BCR application form WP133 and the CBPR Intake questionnaire, identifying similarities and differences, which could be completed by organizations and submitted to both national DPAs in the EU and APEC Accountability Agents to facilitate double certification;*
2) *A mapping of the company policies and associated personal data and privacy program practices and effectiveness tools that must be submitted with this common questionnaire to demonstrate compliance with both systems;*

*On a long term basis, develop:*

3) *A common processor referential mapping the requirements of EU processor BCR and APEC Privacy Recognition for Processors (PRP).*

*Letter of Article 29 Data Protection Working Party Brussels to Ms. Danièle Chatelois, Chair of the APEC Data Privacy Subgroup, 29 May, 2015.*

In Europe, there are also a wide variety of governmental agencies with executive powers spread throughout the EU institutions and at the Member State level (including important local and regional authorities in many Member States). In several cases certain levels of cooperation or coordination have been put into place. Executive agencies of national, local and regional governments, the Council and the Commission – in cooperation with DPAs and the Article 29 Working Party – face challenges to translate the EU data protection framework into practical solutions. These challenges will remain, and perhaps even intensify, under the GDPR. Moreover, in Europe there are many cases of lack of coordination between different governmental entities with regard to data protection, and concerning the data protection implications of policy initiatives in other areas. They would all benefit from a strategy of coordinated action to develop effective policies in order to implement the framework, but also to assess the non-privacy questions that are often involved, such as questions regarding security, safety, and economic development. Regardless of the omnibus regulation on privacy that exists in the EU, individual topics require coordinated responsibilities and actions because (as is the case in the United States) policy decisions involve consultations among many levels of the executive branch. For example, in the case of drone regulation, the implementation of policies developed on the European level (such as the EC Communication on opening the Remotely Piloted Aircraft Systems market) involves multiple European and national executive levels. A similar complexity exists in the field of public health, the financial sector, and many other areas.

In all these cases, governmental and executive agencies have a pro-active interest in addressing privacy and data protection in new circumstances. In parallel with creating a bridge between the institutions involved in supervising and enforcing privacy regulations (see Bridge 1), a similar bridge is proposed between government and executive agencies. This bridge should provide a basis for regular exchanges of information, but also go beyond this and offer transparent platforms for active discussion and practical policy development. In order for this bridge to work, it will be crucial to find the right level of coordination.

We propose that bridges be built between government and executive agencies on both sides of the Atlantic. For example, the White House and the European Commission could improve the coordination between their various departments and directorates. Structures could also be created to improve alignment on the national, local, and regional levels, which – depending on the topic – would require involvement of agencies of the EU Member States. Existing structures such as the EU and US representations in Washington and Brussels can be included and used to build a strong liaison structure. Where helpful new forms of cooperation and coordination between EU Member States can be created (supported and facilitated by the European Union where appropriate). We suggest that as a first step, a central contact point is established in the EU and in the U.S. with the following tasks:

(1) Establishing a permanent liaison between the two jurisdictions;
(2) Identifying within their own jurisdictions legislative or policy developments that could be of interest to share with the other jurisdiction;
(3) Alerting authorities within their own jurisdiction of possible transatlantic privacy issues they have become aware of; and
(4) Organizing joint events to raise awareness.

Building this bridge between the EU and the US will yield a variety of benefits to governments, individuals, and commercial actors. First, it will create a more structured and sustainable platform for better policy coordination by having a one-stop shop mechanism. Second, governments will have the opportunity to share learning about how to apply privacy principles in new technological, scientific and business contexts. Whether or not approaches are identical, the quality of decision-making will no doubt be enhanced by the shared expertise across executive agencies. Third, shared perspective may identify the opportunities to converge policies in specific contexts. This will benefit

the stakeholders in question by streamlining the cost of adopting high-protection privacy practices. Finally, individual data subjects will benefit from a consistent set of privacy protections where services are offered across borders.

Building this bridge will also improve communication/collective thinking and avoid missed opportunities to develop and coordinate the privacy aspects of new policies. The one-stop shop suggested in the bridge would be the first step towards greater engagement and is an essential step for the realization of the other aspects mentioned above.

## 10. COLLABORATING ON AND FUNDING FOR PRIVACY RESEARCH PROGRAMS

Scholars in a wide variety of disciplines – from law to economics, philosophy to mathematics, sociology to computer science – all contribute to evolving conceptions of privacy. To encourage the growth of common perspectives on privacy, this bridge would bring together academics from across the Atlantic to work on joint privacy research projects in a variety of fields. Much of the modern intellectual framework for privacy established in the 1970s and 80s was the product of academic collaboration amongst law scholars in Europe, the United States and other key regions around the world. Now in the face of numerous technical and sociological privacy challenges – including the rise of large-scale analytics and urgent questions about the sociological impact of changes in the handling of personal data – a renewed effort at collaborative research in the transatlantic region is vital. This is especially urgent given the technical innovations that are occurring in the area of privacy and security.

Both security and privacy are complex and fast moving fields with extensive areas of application deployment and academic research. Both require significant technical knowledge to assess the efficacy and applicability of particular methods, tools and techniques. As discussed in Bridge Six, a good example is deidentification: no single technology guarantees the complete anonymization of personal data, especially when they are linkable to other data sets. The developments in this field continue apace and both data custodians and data subjects would benefit from ongoing research regarding the methods of safe data release, their applicability, and their limitations.

De-identification may be applied not only to data sets but also to network communications. In some cases extensive architectures have been established to support anonymous communications,[16] but we need more research to understand the likely evolution of such approaches. It is worth noting that many technical approaches to privacy and deidentification are "dual use" in the sense that both allies and adversaries use and benefit from these systems.

An important alternative to privacy-enhancing technologies based on obscurity, encryption, or anonymization is accountability. There are technological methods for holding organizations accountable so that when they collect and use information, it is possible to determine exactly what happened, and to pinpoint any inappropriate uses. This approach not only leads to transparency but also to the possibility of redress. It is a challenging task to design accountable systems and even more so to have them accepted by the wider digital ecosystem. Moreover, technological methods of accountability would supplement the organizational measures described in Bridge 8.

Providing adequate measures of privacy and security involves many disciplines. Even the best technical security measures can be undermined by social engineering. Thus, it is essential to understand the psychological and social dimensions of digital environments. The most secure systems can be undone by legal, policy and organizational failures as well. Our very notion of what

---

[16] *The Onion Router (TOR https://www.torproject.org ) is one such.*

constitutes data protection, privacy, or a reasonable expectation thereof is a subject of debate. Across the gamut of technology, architecture and policy, there has never been a greater need for collaborative, multidisciplinary engagement.

Global collaboration has been a hallmark of Internet engineering and many related academic disciplines. However, EU and US funding agencies have different policies, procedures and priorities, which inhibit close collaboration. Key barriers include varying research priorities, timing of research solicitations, and limited availability of financial support for cross-border projects (and even outright prohibitions). Of course, researchers on both sides of the Atlantic can work independently on similar problems, exchange views at academic conferences (which are generally global in scope), and read each other's papers. But building teams that work together requires both improved funding coordination and more extensive dialogue between EU and US researchers and funding agencies. And we must include educational programs in the collaborations – this is not just about undertaking research but also about learning from each other.

For cross-border research groups to develop, they must be able to secure funding from their respective governments (or private sector funders) for work that is closely related and on a compatible timeframe. There are concrete steps that government research funding agencies can take to encourage joint research including explicit prioritization of cross-border projects, clear alignment of research topics, and provision in funding solicitations to cover the additional expenses of collaboration. Foundations and corporate funding could play an important role here.

At a time when leading research funding institutions on both sides of the Atlantic have increased their commitment to privacy research and plan to do even more, there is a unique opportunity to promote cross-border, cross-disciplinary collaboration. The US National Science Foundation (NSF), individual European national funding agencies, as well as the European Commission are all supporting research in the area of privacy and security. In particular, there is an increased emphasis on cross-disciplinary research as evidenced by the the NSF's Security and Trustworthy Cyberspace initiative, the EC's Horizon 2020 program, , and others.

Scholars and researchers in all of the disciplines touching on privacy contribute in a variety of ways to society's evolving privacy dialogue: they shape new technologies, develop and evaluate varying legal and regulatory approaches, and document the impact of new personal system on individuals and communities. Academic work is enriched by and informs the work underway in the public and private sectors. Thus, encouraging scholars and researchers to work together in their research will promote common perspectives on these issues that can be shared across the Atlantic.

# V. CONCLUSION

We have analyzed the privacy challenges facing individuals, regulators and companies in the European Union and the United States, described the similarities and differences between EU and US privacy law, and introduced the need for and possibility of privacy bridges as a way to bring the EU and the US closer together in advancing privacy protection for individuals. Our goal has been to provide a framework of practical options that advance strong, globally accepted privacy values in a manner that respects the substantive and procedural differences between the jurisdictions yet moves beyond current impasses. The heart of the Report consists in ten privacy bridges ranging from formalized agreements to user enhancements to best practices to improving EU-US cooperation and coordinating privacy research agendas on a long-term basis. We believe that each of the ten privacy bridges are practical, achievable without legal reform, and, most importantly, will bring about privacy improvements for individuals. While our focus is privacy protection in the transatlantic region, we hope that some of these privacy bridges may prove useful in other regions as well. We invite discussion of these bridges during the Open Session of the 37th International Privacy Conference in Amsterdam and in other venues and by other stakeholders interested in advancing practical solutions to fundamental privacy challenges.

# ANNEXES

## ANNEX I: BIOGRAPHIES OF GROUP MEMBERS

**Participants**

Jean-François Abramatic, French National Institute for Computer Science and Applied Mathematics

Jean-François Abramatic is senior scientist at Inria, the French research institute in Computer Science and Applied Mathematics. His main contribution to "Privacy on the Internet" came from his tenure as Chairman of the World Wide Web Consortium (W3C) from 1996 to 2001.

Bojana Bellamy, Centre for Information Policy Leadership at Hunton & Williams

As the President of Centre for Information Policy Leadership, a global privacy and security think-thank, Bojana brings over 20 years of experience in global data privacy law, policy and compliance, and has held senior roles as global privacy director at Accenture and president of the Board of Directors of IAPP.

Mary Ellen Callahan, Jenner & Block

Mary Ellen Callahan is the Chair of the Jenner & Block Privacy and Information Governance practice, and was the U.S. Department of Homeland Security Chief Privacy Officer from 2009-2012.

Fred Cate, Indiana University Maurer School of Law

Fred H. Cate is Vice President for Research, Distinguished Professor, and C. Ben Dutton Professor of Law at Indiana University, and a Senior Policy Advisor to The Centre for Information Policy Leadership at Hunton & Williams LLP.

Patrick van Eecke, University of Antwerp

Patrick Van Eecke, Professor University of Antwerp, Visiting Professor Queen Mary University, Partner and global co-chair of privacy practice DLA Piper.

Nico van Eijk, Institute for Information Law (IViR) University of Amsterdam (UvA) (Co-chair)

Nico van Eijk is Professor of Media and Telecommunications Law and Director of the Institute for Information Law (IViR, Faculty of Law, University of Amsterdam, http://ivir.nl/medewerkerpagina/eijk).

Elspeth Guild, Centre for European Policy Studies

Elspeth Guild is Associate Senior Research Fellow at CEPS. She is also Jean Monnet Professor ad personam at Queen Mary, University of London as well as at the Radboud University Nijmegen, Netherlands.

Paul de Hert, Vrije Universiteit Brussel (VuB) and Tilburg University

Paul De Hert is an international fundamental rights expert, professor at the Vrije Universiteit Brussels (LSTS) and associated professor at Tilburg University (TILT).

Peter Hustinx, former European Data Protection Supervisor (EDPS)[17]

Christopher Kuner, Vrije Universiteit Brussel (VuB)
Dr. Christopher Kuner is professor of law at the Vrije Universiteit Brussel (VUB) and director of the Brussels Privacy Hub. He is editor-in-chief of the law journal International Data Privacy Law and also teaches at the University of Cambridge, the London School of Economics and Political Science, and the University of Copenhagen.

Deirdre Mulligan, University of California Berkeley
Deirdre K. Mulligan is an Associate Professor at the School of Information, University of California, Berkeley.

Nuala O'Connor, Center for Democracy and Technology
Nuala O'Connor leads the Center for Democracy & Technology, a global NGO focused on human rights and civil liberties in the digital world.

Joel Reidenberg, Fordham University School of Law
Joel R. Reidenberg is the Stanley D. and Nikki Waxberg Chair and Professor of Law at Fordham University where he directs the Fordham Center on Law and Information Policy.

Ira Rubinstein, Information Law Institute, New York University School of Law (Rapporteur)
Ira Rubinstein is Senior Fellow at the Information Law Institute and Adjunct Professor of Law, New York University School of Law, https://its.law.nyu.edu/facultyprofiles/profile.cfm?section=bio&personID=30084.

Peter Schaar, European Academy for Freedom of Information and Data Protection
Peter Schaar, Former German Federal Commissioner for Data Protection and Freedom of Information (2003-2013), now chair of the European Academy for Freedom of Information and Data Protection, Berlin.

Nigel Shadbolt, University of Oxford
Sir Nigel Shadbolt, Professor of Computer Science at the University of Oxford, Principal of Jesus College Oxford and Chairman of the Open Data Institute London.

Sarah Spiekermann, Vienna University of Economics and Business (WU Vienna)
Sarah Spiekermann is a university professor, chairing the Institute for Management Information Systems at Vienna University of Economics and Business and author of the book "Ethical IT Innovation".

David Vladeck, Georgetown University Law Center
David C. Vladeck is a Professor of Law at Georgetown University Law Center, and formerly served as the Director of the Federal Trade Commission's Bureau of Consumer Protection.

Daniel J. Weitzner, Massachusetts Institute of Technology (Co-chair)
Daniel Weitzner is the Director of the MIT CSAIL Decentralized Information Group and teaches Internet public policy in MIT's Computer Science Department. His research includes development of accountable systems architectures to enable the Web to be more responsive to policy requirements.

---

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

**Observer**

Jacob Kohnstamm, Dutch Data Protection Authority (CBP)

Jacob Kohnstamm is the chairman of the Dutch Data Protection Authority (Dutch DPA) and the former chairman of the Article 29 Data Protection Working Party (WP29) and of the Executive Committee of the International Data Protection and Privacy Commissioners Conference.

**Project Support**

Frederik Zuiderveen Borgesius, Institute for Information Law (IViR) University of Amsterdam (UvA)

Dr. Frederik J. Zuiderveen Borgesius, researcher at the IViR Institute for Information Law, University of Amsterdam.

Dominique Hagenauw, Dutch Data Protection Authority (CBP)

Dominique Hagenauw is Senior International Officer at the Dutch Data Protection Authority.

Hielke Hijmans, Vrije Universiteit Brussel and University of Amsterdam (UvA)

Hielke Hijmans is a specialist in European law and has worked for the Dutch government, the European Court of Justice and the European Data Protection Supervisor. He finalizes a doctorate thesis on the task of the EU to ensure internet privacy and data protection.

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

## ANNEX II: LIST OF SUPPORTING ORGANIZATIONS

The following academic and governmental institutions contributed to the travel and administrative/ support expenses related to the meetings:

1. Dutch Data Protection Authority (CBP)
2. European Commission
3. University of Amsterdam, Institute for Information Law (IViR)
4. Massachusetts Institute of Technology Cybersecurity and Internet Policy Research Initiative

As stated in the report, the members of the group are independent experts in the field of privacy and data protection from the European Union and the United States. They have not received any payments from the project for their participation (except the reimbursement of their travel/hotel and administrative/support costs for the co-chairs and the rapporteur.)

## ANNEX III: LIST OF GROUP MEETINGS

1. April 28-29, 2014, Amsterdam
2. September 22-23, Washington, DC
3. December 9-10, 2014, Brussels
4. March 23-24, 2015, New York, New York
5. June 15-16, 2015, Paris

The group has invited various guests to discuss aspects of the project or to give presentations. Those who agreed to have their names mentioned are (in alphabetic order):

Jan Philipp Albrecht, Member, Committee on Civil Liberties, Justice and Home Affairs (LIBE) and Rapporteur of the European Parliament for the data protection regulation
Julie Brill, Commissioner, Federal Trade Commission
Marjory Blumenthal, Executive Director of the President's Council of Advisors on Science and Technology (PCAST)
Justin Brookman, Privacy Director, Center for Democracy and Technology (CDT)
Chris Calabrese, Legislative Counsel, American Civil Liberties Union
Stephen Deadman, Group Privacy Officer, Vodafone
David Edelman, Senior Advisor for Internet, Innovation, & Privacy Policy, Office of Science and Technology Policy and the National Economic Council
Erin Egan, Vice President and Chief Privacy Officer, Policy, Facebook
John Frank, Vice President and Deputy General Counsel, Microsoft
Morton Halperin, Senior Advisor, Open Society Foundation
Caroline Louveaux, Chief Privacy Officer, Mastercard
Ginger McCall, Associate Director, Electronic Privacy Information Center (EPIC)
John B. Morris, Jr., Associate Administrator and Director of Internet Policy, Office of Policy Analysis and Development, National Telecommunications and Information Administration
(NTIA)
Paul F. Nemitz, Director for Fundamental rights and Union citizenship in the Justice Directorate-General (DG Justice) European Commission
Jules Polonetsky, Executive Director and Co-Chair, Future of Privacy Forum
Harriet Pearson, Partner, Hogan Lovells
Florence Raynal, Commission nationale de l'informatique et des libertés (CNIL)
Tim Sparapani, Vice President of Law, Policy, and Government Relations, Applications Developers Alliance
Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation (EFF)
Florian Toma, Chief Privacy Officer, Accenture
Peggy Valcke, KU Leuven and Member, Google Advisory Committee
Corrine Yu, Senior Counsel and Managing Policy Director, Leadership Council on Civil Rights)

## ANNEX IV: LIST OF GLOBAL NETWORK INITIATIVE IMPLEMENTATION GUIDELINES

**Privacy**

**Data Collection**
Participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks.

**Government Demands, Laws and Regulations**
Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government demands") that are issued regarding privacy online.

Participating companies will also encourage government demands that are consistent with international laws and standards on privacy. This includes engaging proactively with governments to reach a shared understanding of how government demands can be issued and implemented in a manner consistent with the Principles.

Participating companies will adopt policies and procedures which set out how the company will assess and respond to government demands for disclosure of personal information. When required to provide personal information to governmental authorities, participating companies will:
- Narrowly interpret and implement government demands that compromise privacy.
- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.

***Application Guidance:*** *Overbroad could mean, for example, where more personal information is requested than would be reasonably expected based on the asserted purpose of the request.*
- Request clear communications, preferably in writing, that explains the legal basis for government demands for personal information including the name of the requesting government entity and the name, title and signature of the authorized official.

***Application Guidance:*** *Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.*
- Require that governments follow established domestic legal processes when they are seeking access to personal information.
- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that Country.

***Application Guidance:*** *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*
- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.

***Application Guidance:*** *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.*

***Application Guidance:*** *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

**Communications with Users**

Participating companies will seek to operate in a transparent manner when required to provide personal information to governments. To achieve this, participating companies will:

***Application Guidance:*** *Participating companies will work with the Organization to raise awareness among users regarding their choices for protecting the privacy of their personal information and the importance of company data practices in making those choices.*

- Disclose to users in clear language what generally applicable government laws and policies require the participating company to provide personal information to government authorities, unless such disclosure is unlawful.
- Disclose to users in clear language what personal information the participating company collects, and the participating company's policies and procedures for responding to government demands for personal information.
- Assess on an ongoing basis measures to support user transparency, in an effective manner, regarding the company's data collection, storage, and retention practices.

Source: http://globalnetworkinitiative.org/sites/default/files/GNI_-_Implementation_Guidelines_1_.pdf

## ANNEX V: BASIC ELEMENTS OF BREACH NOTIFICATION LAWS

As to the **scope of the notification duty**, most legal instruments require notification for any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data" (ePrivacy Directive), "any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein" (Trust Services Regulation), any "incidents having a major impact on the security of the core services they provide" (draft NIS Directive) or "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Draft GDPR). In the U.S., there are states that require notification whenever there has been unauthorized access to acquisition (14 states in total), and some states that require notification only when there is the risk or knowledge of harm. In HIPAA, a risk assessment should be applied to determine what notification is required.

As to the **time frame** of the notification, some laws (including the Draft GDPR) refer to the duty to notify "without undue delay but in any event within 24 hours after having become aware of it"(Trust Services Regulation), "without undue delay" (ePrivacy directive), "without undue delay and, where feasible, not later than 72 hours after having become aware of it" (Draft GDPR); in the U.S., notification to the individual is to be no later than 30 (Florida) to 60 (HIPAA/HITECH) days after becoming aware of the unauthorized access; notification to the affected companies should be as soon as possible.

As to the **recipients of the notification**, in the EU, some laws/draft laws introduce a triple approach: first notifying a competent national authority (national body (ePrivacy Directive), supervisory body (Trust Services Regulation), or supervisory authority (Draft GDPR)). In case the breach is "likely to adversely affect a natural or legal person" (Trust Services Regulation), or "likely to result in a high risk for the rights and freedoms of individuals" (Draft GDPR), the involved person should be informed. This could be a natural or legal person (Trust Services Regulation), the subscriber or individual (ePrivacy Directive), or the data subject (Draft GDPR). Thirdly, some laws/ draft laws require that in case the "disclosure of the breach of security or loss of integrity is in the public interest" (Trust Services Regulation) the general public should be notified about the breach; in the US state laws, notification is at least to the affected individuals; in about 20 states, notification is required to state officials as well. In HIPAA, notification is required to individuals as well as the Office for Civil Rights in the Department of Health and Human Services.

Under certain circumstances, **no notification** to the individual would be required. For example, this would be the case "if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access it." (ePrivacy Directive). HIPAA/HITECH applies a risk assessment.

As to the **contents of notification**, in both regions, the law typically requires firms to describe the nature of the personal data breach, the data elements affected, contact points, measures to mitigate the possible adverse effects of the personal data breach, the number of data subjects concerned, and the consequences of the personal data breach.