
Testimony and Statement of

Marc ROTENBERG, President
Electronic Privacy Information Center (EPIC),
Adjunct Professor, Georgetown University Law Center

"The Reform of the EU Data Protection Framework—
Building Trust in a Digital and Global World"

Before the

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

Room JAN Q42
European Parliament
Brussels, Belgium
10 October 2012

**SUMMARY – THE CHALLENGE OF DATA PROTECTION**

EPIC supports the Reform of the EU Data Protection Framework and believes that this process will establish important new protections for individuals in Europe and around the world. The General Data Protection Regulation achieves several important goals. First, it simplifies the existing framework of European privacy laws. Second, it strengthens rights for consumers. Third, it clarifies legal authority for data privacy agencies. Fourth, it updates privacy protections in light of new data collection practices. Fifth, it reaffirms a fundamental right of great importance.

The Reform of the EU Data Protection Framework is broadly supported by consumer organizations in the United States. As more than twenty US organizations have recently stated, "we believe that the promotion of stronger privacy standards in Europe will benefit consumers around the globe." We join with consumer and privacy organizations across Europe, including BEUC, Privacy International, EDRi, and others, who have also expressed support.

While we support the effort, let us also be clear about the enormous challenge for data protection today. When the Directive was adopted in 1995 there was no commercial profiling of Internet users; there was hardly any commercial use of the Internet.

Biometric identification was mostly limited to fingerprints and criminals. The details contained on identity documents, such as passports and drivers licenses, could not be obtained unless they were actually removed from a wallet or purse. Surveillance cameras were typically found in banks not street corners or residential neighborhoods. Governments did not spend billions of dollars on new technologies that made it possible to view people, suspected of no crime, stripped naked. There was far less integration of personal data provided across many distinct services by a single company. Children were not encouraged to post personal information online, nor did businesses represent that the information would only be shared with family and friends while simultaneously disclosing the data to business partners, application developers, and others.

There have also been substantial changes in the architecture of our networked society. In particular, the movement of the individual's data to the cloud raises profound privacy and security issues. The revolution that once promised greater user control over technology now seems to be moving in opposite direction. No longer is our data in our possession. And the traditional legal protections that would protect our data in our homes and offices do not protect the data that is now stored in the "cloud," *i.e.* the remote servers of large Internet firms that are subject to the authorities of police and intelligence agencies.

Governments have moved slowly in response to these new challenges. In the United States, we still have not updated the 25 year-old Electronic Communications Privacy Act to take account of cloud computing. Instead, the most recent amendments to the privacy law expanded law enforcement access to user data under the Patriot Act and also under FISA Amendments Act. As a consequence, user data stored in cloud-based services, particularly the data of non-US citizens, is easily accessible by US agencies for a wide variety of purposes.

There is also some progress in the United States. The President has put forward a Consumer Privacy Bill of Rights, a good set of principles that reflect many well-known privacy values. The Federal Trade Commission has entered into important settlements with major Internet companies under its authority to investigate unfair and deceptive trade practices. But the President's Bill of Rights lacks legal force, and questions remain about the FTC's willingness to enforce its own consent orders.

And of course the EU Data Protection Regulation is not without its flaws. Substituting a single "one stop shop" for the many competencies of data protection agencies may place consumers at new risk precisely when the expertise of these national organizations has become so crucial. And beyond the Regulation of the private sector, there are also serious concerns about the new Directive for the processing of data for police activity. In many respects, the Directive lacks the provisions for meaningful protections and questions about transparency remain. And we know that the challenges of data protections in both spheres will only increase in the years ahead.

This is why the topic of our panel – "Standards for Effective Protection in the Global Context" – is now crucial. The protection of privacy is a global challenge, and the problems facing consumers around the globe is a common challenge. Among citizens, consumers, and users of new Internet-based services, there is far more agreement than disagreement about the need to protect privacy.

- The law should be updated and legal rights should be enforced
- Privacy policies should be honored and companies should be held accountable
- Organizations that collect personal data should protect that data
- Transparency of processing is critical for privacy protection
- Techniques to protect privacy should be adopted
- Special protections for children are necessary and appropriate
- Most fundamentally, individuals should remain in control of their personal information, particularly when it is held by others.

This is the key to "building trust in a digital and global world," the theme of our conference this week. Trust exists where data protection is established and enforced.

Let us also say a few words about the importance of making these decisions in the context of Constitutional democracies. Several years ago, more than a hundred civil society organizations and privacy experts joined together in support of a declaration affirming international instruments that protect privacy, and setting out specific recommendations. The Declaration reaffirmed the EU privacy framework, and the importance of independent data protection agencies.

The Madrid Privacy Declaration ends with a call for a new international "framework for privacy protection, with the full participation of civil society, that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions." The data protection reform efforts now underway in the European Union reflect this spirit and deserve support in Europe and around the world

**Introduction**

On behalf of EPIC, I would like to thank Chairman Lopez Aguilar, the Rapporteur Jan Albrecht, the members of the LIBE Committee, and the representatives of the National Parliament for the opportunity to speak with you today. My name is Marc Rotenberg, and I am the President and Executive Director of the Electronic Privacy Information Center. I also teach Information Privacy Law and Open Government Law at the Georgetown University Law Center. EPIC is a public interest research center in Washington, D.C., established to focus public attention on emerging civil liberties issues. EPIC has worked to promote privacy and human rights since our founding in 1994. We work closely with civil society organizations in the United States and around the world. In two weeks, EPIC will host the 25th Public Voice conference, in conjunction with the annual meeting of the International Conference on Privacy and Data Protection in Uruguay.

I will start by discussing the general importance of the Regulation. Then, because this Session addresses data protection in a global context, I will focus on the Regulation's international transfer mechanism, as well as the international context in which the Regulation arises.

EPIC supports the EU General Data Protection Regulation and believes that it provides important new protections for the privacy and security of consumers. The Regulation achieves three important goals. First, it simplifies the existing network of European privacy laws. Second, it strengthens enforceable legal rights for consumers, creates more definitive legal authority for government privacy agencies, and identifies new legal responsibilities for businesses. Finally, it refocuses the privacy discussion on the rights of the consumer, rather than the rights of businesses. EPIC therefore urges the Committee to adopt the Regulation.

Given the global nature of the digital economy, the Regulation's provision for international data transfer is necessary. But the Committee should ensure that data is not transferred to a jurisdiction that does not provide adequate protections for personal data. In particular, the Regulation should not allow transfer to a jurisdiction that has already been recognized by the European Commission as inadequate, and the Regulation should avoid relying on protections that are not provided in a legally-enforceable document. In particular, the Committee should ensure that the international cooperation mechanism does not allow enforcement to be undermined by a self-regulatory or co-regulatory process that does not respect fundamental rights.

The Regulation's approach to privacy contrasts favorably with that of the United States, which has no general commercial privacy law. In this environment, the Federal Trade Commission has emerged as the de facto privacy protection agency. The FTC has succeeded in obtaining consent orders with several major companies, and has even enforced an order in one case. However, other recent failures to act against Google and Facebook reveal the weaknesses in the US approach.

Other international privacy agreements are important and worth considering as the Committee contemplates the proposed reform. For example, EPIC believes that the OECD Privacy Guidelines are one of the clearest articulations of the Fair Information Practices available. They were the first internationally agreed-upon set of privacy principles and have provided core principles for data protection legislation and codes for OECD and non-OECD countries alike. The core principles of the Privacy Guidelines still provide an ideal framework to protect data and their full implementation should be promoted. Any reconsideration of the 1980 Privacy Guidelines must be extremely careful not to weaken the data protection provided by the original Privacy Guidelines. EPIC also helped develop the Madrid Privacy Declaration, which reiterates the obligation of OECD countries to follow the 1980 Privacy Guidelines, identifies new challenges, and calls for concrete actions from all countries. Finally, we fully support the Council of Europe Convention 108 and have urged the United States to ratify it.

## II. The EU General Data Protection Regulation Provides Important New Protections for the Privacy and Security of Consumers

### A. The Regulation Simplifies the Existing Network of European Privacy Laws

One of the great advantages of the Regulation is its simplification of the landscape of European privacy law. While the 1995 Data Protection Directive[1] laid the groundwork for a privacy regime that included personal data processing activities in EU Member States in both the public and private sectors, it still allowed each member state to establish its own set of privacy laws. Twenty seven different implementations of the 1995 rules have resulted in "divergences in enforcement" methods, and the proposed Regulation helps to better coordinate these disparate regulatory schemes. The Parliament has predicted that the new, single law will eliminate the costly administrative burdens that result from having to coordinate 27 different enforcement methods, allowing businesses to save an estimated €2.3 billion per year.[2]

The Regulation is applicable to all non-EU companies (even those without EU presence). Thus, if a business's data processing includes the data of EU residents, international companies must create a corporate infrastructure—for instance, a European Data Privacy officer —to ensure compliance with EU law. The Regulation also creates a uniform set of sanctions, so that in an increasingly global online economy, businesses can structure their privacy policies in full knowledge of the ramifications of breaching the law. These sanctions are scaled according to the seriousness of the violation. For example, under the proposed Regulation, national supervisory authorities may send warning letters to businesses for their first breach of the law. Less serious violations—for example, if a company were to charge a user for requesting his personal data—incur sanctions starting at €250,000 or up to 0.5% of the business's total annual turnover.[3] For more serious violations—for example, processing sensitive data without an individual's

---

[1] Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[2] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=en&guiLanguage=en

[3] *See* Article 79.4.

consent—supervisory authorities have the authority to impose penalties of up to €1 million or a full 2% of annual turnover.[4]

## B. The Regulation Strengthens Enforceable Legal Rights for Consumers, Creates More Definitive Legal Authority for Government Privacy Agencies, and Identifies New Legal Responsibilities for Businesses

EPIC favors the approach of the Regulation, which creates legally-enforceable rights, over a self-regulatory approach, which is inherently limited by the self-interest that controllers and processors have in exploiting personal data. Codes of conduct and standards, while helpful to lawmakers, are not sufficient to create stable consumer confidence in a robust online marketplace. Better data protection rules mean that a consumer can be more confident about his personal data is treated. These stronger data protection rules will in turn help increase trust in online services, so that a consumer is able to use new technologies more confidently and can reap the benefits of participation in an international market. Clearly defined and delineated rules for the free movement of data will also help businesses grow within a data protection framework that can be trusted.

Several of the Regulation's provisions are particularly important. For example, the Regulation rejects a "notice and choice" approach to privacy protection. Invariably such mechanisms operate as "waivers" or "disclaimers," essentially allowing companies to do whatever they wish with the personal data that they collect. In fact, notice and choice has been considered a failed model by both privacy scholars[5] and even now the Federal Trade Commission. "[T]he 'notice-and choice model,'" the FTC noted, "which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand." [6]

EPIC recognizes that, in some circumstances, consumers might want to give informed consent to have the business collect their personal data. It is therefore important that Article 7 establishes necessary conditions for meaningful consent, particularly that the burden of proof for consent rest on the controller. We also support the inclusion of a consumer's right to withdraw consent at any time, as well as the right to have one's data deleted once there is no longer a business relationship. However, the conditions for consent specified in Article 7 could allow for the possibility of a single, "blanket" consent provision that provides consent to data processing in perpetuity. Such a mechanism is not meaningful as consumers do not know which future acts the consent enables. We encourage the Commission to clarify that blanket consent provisions do not satisfy the consent requirement of the Regulation.

Similarly, EPIC supports the Regulation's promotion of privacy by design and privacy enhancing techniques.[7] The Regulation anticipates the use of privacy by design from a business'

---

[4] *See* Article 79.6.
[5] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140(4) DAEDALUS 32, 36 (2011) *available at* http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf.
[6] FED'L TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 2 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[7] Article 23.1.

earliest stages of personal data protection planning, through the use of that data as part of the business model, through the ultimate disposal of that data. Key for EPIC is the belief that genuine Privacy Enhancing Techniques will minimize or eliminate the collection of personally identifiable information, such that users are able to obtain services without placing at risk their personal data.

EPIC are also encouraged by the incorporation Articles 19 and 20, which describe the limitations on businesses with regard to user profiling.[8] The coverage of profiling is particularly important in light of recent reports that detail the ways in which consumers are sorted according to hidden criteria, and then offered better or worse services based on these profiles.[9] Opaque industry practices result in consumers remaining largely unaware of the monitoring of their online behavior, the security of this information and the extent to which this information is kept confidential. Industry practices, in the absence of strong privacy principles, also prevent users from exercising any meaningful control over their personal data that is obtained. EPIC supports limitations on profiling, and requests that the Committee include a mechanism for consumers to find out whether they are being profiled, to obtain a copy of their profile, and to discover specific information about the techniques and numeric values associated with the profiling.

### C. The Regulation Refocuses the Privacy Discussion on the Rights of the Consumer, Rather than the Rights of Businesses

EPIC supports the Regulation's focus on the rights of data subjects through the provisions on transparency, data breach notification, data erasure, and data portability. The transparency mechanism requires a data controller to provide to the data subject, within one month and free of charge, the personal data it has stored. This information has to be provided in an intelligible form, using clear and plain language. The Regulation also requires that data collectors notify supervisory authorities and data subjects of a breach. In either case, the data collector must submit notice "without undue delay and, where feasible, not later than 24 hours after becoming aware of it . . . ."[10] When controllers are responsible for notifying data subjects, they must include recommendations on how the data subjects can protect themselves from harm.[11] Under the right of erasure, sometimes called the "right to be forgotten,"[12] the data subject can require the collector to erase personal data related to him or her and to cease further dissemination of the data.[13] Under the right of portability, individuals can transfer their data from one automated, electronic system to another.[14] These provisions reflect a proper focus on the rights of consumers.

---

[8] Article 19; Article 20.
[9] https://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html?pagewanted=all&_r=0;
http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html
[10] Art. 31.
[11] Art. 32(2). However, Art. 32(3) specifies that such notification is not necessary where the data has been encrypted such that it is rendered unintelligible to any person who is not authorized to access it.
[12] *See* GDPR at 25.
[13] Art. 17
[14] Art. 18(2).

## III. The Committee Should Ensure that the International Transfer Provision is not Used to Undermine the Other Provisions of the Regulation

Chapter V of the Regulation addresses international transfers of personal data. These provisions clarify the conditions that must be satisfied for a transfer of personal data from the EU to a non-EU country. First, the Regulation permits data transfers if the Commission has determined that the laws of the recipient "ensures and adequate level of protection" with respect to the transfer of personal data.[15] Where the Commission has not explicitly adopted an adequacy decision, the Directive provides that the Commission shall determine adequacy by examining the legal regime/system of the recipient, the quality of the existing data protection authority, and the international commitments entered into by the recipient.[16]

In the absence of any adequacy determination, the Regulation allows member states to permit data transfers if appropriate safeguards exist in a legally-binding instrument.[17] Legally-binding instruments include binding corporate rules, standard data protection clauses adopted by the Commission or a supervisory authority,[18] and contractual clauses between a controller or processor and the data recipient, if authorized by the supervisory authority.[19] In the absence of a legally-binding instrument, the controller or processor must receive prior approval from the supervisory authority.[20]

The Regulation also contains a derogation allowing data to be transferred in the absence of either an adequacy determination or appropriate safeguards. The derogation enumerates eight circumstances, including where the data subject consents to the transfer, where the transfer is necessary for the public interest, where the transfer is necessary to protect the vital interests of the data subject or another person, and where transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor.[21] Finally, the Regulation encourages the Commission and member states to develop international cooperation mechanisms to facilitate international enforcement.[22]

Given the global nature of the digital economy, the Regulation's provision for international data transfer is necessary. EPIC agrees with the Commission's finding that "[t]he new rules will create advantages for EU companies in global competition, as they will be able to offer their customers assurances of strong data protection whilst operating in a simpler regulatory environment."[23] The Committee should ensure, however, that the international transfer

---

[15] Article 41.1
[16] Article 41.2
[17] Article 42.
[18] "'supervisory authority'" is defined as "a public authority which is established by a Member State in accordance with Article 46." See Article 4(19).
[19] Article 42.2(a)-(d)
[20] Article 42.5
[21] Article 44
[22] Article 38.1
[23] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=en&guiLanguage=en

mechanism does not facilitate the transfer of personal data to less-protective jurisdictions and thereby weaken the protections provided in the rest of the Regulation.

Specifically, derogation (h) in Article 44 allows for data transfer in the absence of an adequacy determination or appropriate safeguards if the transfer is necessary to fulfill the "legitimate interests" of the data controller or processor.[24] The "legitimate interests" derogation requires that the transfer cannot be "frequent" or "massive," and that the processor or controller must provide appropriate safeguards based a documented assessment of the circumstances surrounding the transfer. Nevertheless, the derogation is broad. Given that Article 44 already allows controllers or processors to transfer data (1) with the consent of the data subject; (2) for the performance of a contract; (3) for "important grounds of public interest"; (4) for the exercise or defense of legal claims; and (5) to protect the vital interests of the subject or another person. Thus, it is hard to see what is added by the "legitimate interests" exception, other than a catch-all provision that threatens to undermine the effectiveness of the Regulations protections.

Similarly, the Committee should scrutinize the Regulation's allowance for data transfers where rights are secured through voluntary codes of conduct or self-regulatory approaches. The adequacy mechanism is likely to be tested by the privacy multistakeholder process of the United States, which aims to turn the Consumer Privacy Bill of Rights into codes of conduct that can be voluntarily adopted by data controllers or processors, and enforced by the Federal Trade Commission. Although the process is still in its early stages, it is unlikely to produce a set of protections equal to those contained in the Regulation. And self-regulation may also be tested by Article 42.5, which provides for transfers in the absence of both an adequacy determination and a legally-binding instrument if the processor or controller obtains authorization from a supervisory authority.[25] This provision might encourage controllers or processors to transfer data using codes of conduct, rather than through legally-binding mechanisms.

Scrutinizing the international transfer mechanism is particularly important in light of the failures of the U.S.-EU Safe Harbor Framework. Academic experts have criticized the Safe Harbor Framework, noting that almost a decade passed before the Federal Trade Commission brought an enforcement action against a U.S. company with respect to the Safe Harbor.[26] Furthermore, three studies of the Safe Harbor Framework, conducted in 2001, 2004, and 2008, found numerous deficiencies, with the most recent study finding that "the growing number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers."[27] In 2010, the Data Protection and Privacy Commissioner for the German state of ____ demanded termination of the Safe Harbor agreement, citing low levels of enforcement by the United States.[28] Given this history, the Committee should exercise a higher level of caution in reviewing the adequacy of the US privacy regime.

## IV. The Regulation's Approach to Privacy Contrasts Favorably with that of the United States, which Lacks a General Commercial Privacy Law

[24] Article 44.1(h).
[25] Article 42.5
[26] http://writ.news.findlaw.com/ramasastry/20091117.html
[27] http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf at 18
[28] *Id.* at 19.

The United States lacks a comprehensive privacy regime. Instead, myriad laws and agencies independently regulate various areas of privacy. For the personal information of consumers, the Federal Trade Commission ("FTC") has emerged in recent years at the *de facto* privacy protection agency. Its statutory mandate is to promote consumer protection and eliminate anti-competitive business practices.

## A. FTC Settlements with Facebook and Google

There are various strengths and weaknesses of the Federal Trade Commission as a privacy agency. First, the FTC is an independent agency; it is bipartisan and does not answer to the President. As such, it has the ability to investigate privacy violations and enforce sanctions without being weighted down by partisan politics. This gives the Commission's decisions a legitimacy similar to that of an impartial court. While any given commissioner may have party affiliations and biases, the Commission as a whole is respected for its bipartisanship.

Recently, and with EPIC's prompting, the FTC has undertaken substantial investigations and enforcement actions against Facebook, Google, and other Internet firms for privacy violations. The resulting consent orders show how a robust agency can enforce consumer privacy protections.

In 2009, EPIC and other public interest organizations filed a complaint with the FTC about Facebook's policies and practices.[29] Facebook instituted changes to its settings, without user notification or consent that compromised users' privacy. The FTC investigated the matter and in 2011 it issued a formal complaint against Facebook and a consent order.

The FTC outlined numerous privacy violations committed by Facebook. Facebook made previously private information, such as lists of friends, public without user consent. It gave third-party apps access to nearly all of a user's personal data, even when the user tried to restrict access to certain data. Facebook shared users' information with advertisers despite promising that it would not. Despite claims to the contrary, Facebook did not comply with the Safe Harbor Framework governing data transfers between the U.S. and the E.U.

The FTC ordered Facebook to give its users a prominent notice and obtain affirmative consent before sharing personal information. Facebook is prohibited from misrepresenting its privacy and security practices. When a user deletes their account, Facebook must remove their user information within 30 days. FTC demanded that Facebook both establish a comprehensive privacy program and submit to independent privacy audits for the next 20 years.

Google's privacy violations are also a subject of FTC investigation. In 2010, EPIC filed a complaint with the FTC highlighting how Google's social networking services threatened the privacy of Gmail users.[30] The FTC determined that Google engaged in unfair and deceptive trade practices by manipulating users' privacy without their consent. The resulting FTC consent order

[29] For more information, see EPIC: FTC Facebook Settlement at http://epic.org/privacy/ftc/facebook/.
[30] For more information, see EPIC: EPIC v. FTC (Enforcement of the Google Consent Order) at http://epic.org/privacy/ftc/google/consent-order.html.

established new privacy safeguards for all Google products and services. FTC barred Google from misrepresenting the company's privacy practices, ordered Google to obtain users' consent before disclosing their data, and required Google to obtain regular privacy audits.

In November 2011, the FTC finalized its consent order with Google, and in August 2012, the FTC finalized its consent order with Facebook. Both orders prohibit the companies from future privacy misrepresentations, require them to implement a comprehensive privacy program, and calls for regular, independent privacy audits for the next 20 years.

After the consent order with Google in 2011, news reports revealed that Google bypassed privacy settings in Apple's Safari web browser in order to track users and target advertisements. The FTC deemed this to be a violation of the consent order and fined Google $22.5 million, the largest civil penalty in the history of the FTC.[31]

## B. Lack of FTC Enforcement, Consideration of Public Comments; Absence of Safeguards for the Cloud

In other cases, however, the FTC has not acted to prevent violations of its consent orders. Earlier this year Google announced that it would consolidate its users' data for all of Google's services, including Gmail, YouTube, and Android.[32] Rather than allowing users to have differing degrees of privacy and profiles across different platforms, Google forced its users to use a single merged profile. While many Attorneys General in United States expressed concern about the proposal and the French Data Protection Agency warned Google that this proposed change violates E.U. privacy laws,[33] the FTC refused to act to enforce its own consent order. EPIC filed a lawsuit to force the agency to act, but a federal court held that the FTC's enforcement decisions were not judicially reviewable.[34]

Recently, Facebook announced a new business arrangement with the web-tracking firm Datalogix. The deal allows Datalogix to track the activities of Facebook users in their offline activity and to report back to Facebook so as to assess the effectiveness of Facebook advertising. Under pressure from its new shareholders, Facebook seeks new ways to trade on its users' private information. Although this new disclosure of user information with the informed consent of the user appears to violate FTC's consent order with Facebook, the Commission has yet to take action.[35]

---

[31] Claire Cain Miller, "F.T.C. Fines Google $22.5 Million for Safari Privacy Violations," New York Times Bits Blog, Aug. 9, 2012, http://bits.blogs.nytimes.com/2012/08/09/f-t-c-fines-google-22-5-million-for-safari-privacy-violations/.

[32] For more information, see EPIC: EPIC v. FTC (Enforcement of the Google Consent Order) at http://epic.org/privacy/ftc/google/consent-order.html.

[33] Letter from Isabelle Falque-Pierrotin, President of Commission Nationale de l'Informatique et des Libertes, to Larry Page, CEO of Google Inc., on Feb. 27, 2012, available at http://epic.org/privacy/ftc/google/Courrier-Google-CE121115-27-02-2012.pdf

[34] See http://epic.org/privacy/ftc/google/consent-order.html.

[35] For more information, see EPIC: Facebook and Datalogix, at http://epic.org/privacy/facebook/facebook_and_datalogix.html.

Furthermore, the Federal Trade Commission refuses to consider any public comments for how to improve the proposed settlements even when it has formally requested comments from the public. For example, in response to FTC's call for comments on the Facebook settlement, many interested parties submitted recommendations to the Commission. EPIC said that although the settlement is far-reaching and comprehensive, it could be improved.[36] EPIC submitted over 30 pages of comments containing detailed suggestions,[37] but the FTC declined to adopt any modifications to the ensuing consent order. The Federal Trade Commission has adopted a similar approacg with the settlements on Google and Myspace, refusing even to recommend that companies subject to a "comprehensive privacy program" adopt the principles set out in the President's Consumer Privacy Bill of Rights.

Apart from the Federal Trade Commission's role in certain consumer privacy matters, there are also broad concerns about the growing reliance on cloud computing services. There is a fundamental change taking place in the architecture of the Internet and much of the computing power, data, and application software that previously resided with the user is now migrating back toward the center of the network. In particular, the personal data that was once stored on the computers in our homes and offices is now being stored on the remote servers of Internet firms.

US privacy laws should reflect this new reality but the Electronic Privacy Communications Privacy Act, adopted in 1986, treats information stored online for more than 180 days, including private communications, as essentially abandoned, entitled to only the most legal minimal protections. In fact access to sored information, particularly of non-US citizens, by US police agencies has been made easier as a result of the passage of the Patriot Act and the FISA Amendments Act. Large amounts of private data may be swept up from cloud service providers in the United States without any suspicion of criminal conduct. Remarkably, even the very weak legal provisions of the PNR arrangement do not apply to this much larger and more rapidly growing area of commercial activity.

## V. International Standards for Effective Protection Include the OECD Privacy Guidelines, the Council of Europe Convention 108, and the Madrid Privacy Declaration

We are asked for this panel to consider "Data Protection in the Global Context – Standards for Effective Protection." For this reason, several other international privacy frameworks are worth noting.

### A. The OECD Privacy Guidelines

[36] For more information, see EPIC: FTC Facebook Settlement at http://epic.org/privacy/ftc/facebook/.

[37] See https://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf. First, we recommended that the FTC order Facebook to restore its original privacy settings. Second, Facebook users should be able to access all of the data that Facebook keeps about them. We are pleased that the proposed EU regulation includes such a right of access. Third, Facebook should be prohibited from using facial recognition without users' consent. Facebook recently suspended its facial recognition software in both the E.U. and the U.S. in response to privacy violation complaints. However, there is nothing barring Facebook from restarting this program in the U.S. Fourth, in the interest of transparency, Facebook's regular privacy audit reports should be available to the public. Finally, we also called on the FTC to prevent Facebook from secretly tracking users across the web.

The 1980 OECD Privacy Guidelines were the first internationally agreed-upon set of privacy principles and have been extremely significant and influential as a policy framework. [38] The Privacy Guidelines led directly to adoption of national laws in many countries, new business practices, and professional codes of conduct.

The Privacy Guidelines are an example of how a smart legal regime can provide robust data protection while promoting innovation and competition. Several key factors lead to the success of the Privacy Guidelines. First, the Guidelines were forward-looking. There were bold and ambitious. They took on an emerging problem that was not well understood by the general public. Second, the Guidelines were technologically neutral. The OECD took on a challenge infused with technology and, rather than attempting to define, describe, or regulate the technology, chose instead to focus on the rights and responsibilities of the various participants in the collection and use of personal data. The Guidelines work as well for networks based on mainframe computers and acoustic couplers as they do for mobile devices and broadband Internet. Additionally, the Guidelines had the right level of specificity. In this respect, the Guidelines passed the Goldilocks test; they were neither "too hot" nor "too cold." A more specific statement could have been confusing. A more general statement would have been too vague and lacked practical effects.

Finally, the OECD Guidelines reflect the central goal of protecting privacy to enable the free flow of information. Jan Frees said this famously many years ago, and it is still the best way to understand the relationship between data protection and the free flow of information. Privacy protection enables the trust and confidence that enables consumers to participate in new networks environments, to reveal information that they otherwise are reluctant to share. In the absence of privacy protection, information would flow less freely. It appears as a paradox; to many it is counter-intuitive. It remains still the core principle of an effective privacy framework.

At the same time, the OECD Guidelines lack at least two critical building blocs for effective data protection that are found in the EU Directive and will be established in the Regulation – a legal framework that provides the basis to pursue legal rights and the institutions of data protection, including independent agencies specifically dedicated to the task of data protection and committees with the expertise to evaluate emerging privacy risks and to make appropriate recommendations. We favor the simple, principle-based approach of the OECD Privacy Guidelines but recognize that effective data protection requires also a legal basis and supervisory authorities.

## B. The Council of Europe Convention 108

We also consider the important Council of Europe Convention 108 and the possibility that the United States could begin the process of consideration and ratification. Developed over thirty years ago, The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data sought to secure the individual's rights and freedoms concerning "his right to privacy, with regard to automatic processing of personal data relating to

38 http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

him."[39] Convention 108 was developed by those who saw the promise of new computer technology but also recognized the risk to fundamental human rights. Their aim was to ensure that the rights of the individual would be protected even as governments and private organizations took advantage of new systems of automation.

The Convention still remains the only binding international legal instrument with a worldwide scope of application in the field of data privacy, open to any country, including countries which are not Members of the Council of Europe. The Convention contains important data protection principles, including data minimization, rights of transparency and access, and limitations on processing of sensitive data.[40]

Currently, 44 countries have ratified Convention 108.[41] EPIC has recommended to US Secretary of State Hilary Clinton that the United States begin the process of ratification, stating that "[o]ver the long term, we must move toward a global framework for privacy for a global world. Convention 108 provides the basis for this framework."[42] We see Convention 108 as providing a basis for the United States and other countries to enter into an enforceable framework for privacy protection.

### C. The Madrid Privacy Declaration

Finally, we would like to draw your attention to the Madrid Privacy Declaration,[43] which reaffirms international privacy instruments, identifies new challenges, and calls for concrete actions from all countries. The new challenges include the increased use of surveillance technology, new surveillance practices (e.g. behavioral tracking), and the consolidation of Internet-based services. These challenges threaten our associated freedoms and strengthen the need for strong data protection.

The Madrid Declaration also calls for a moratorium on the development of new systems of mass surveillance, such as airport body scanners, biometric identifiers, and RFID tags, subject to a "full and transparent evaluation by independent authorities" and democratic debate. The Declaration also urges that the discussion an international framework for privacy protection take place, "with the full participation of civil society, based on the rule of law, respect for fundamental human rights and democratic debate."

The Madrid Declaration is a powerful statement from civil society and privacy experts about the need to safeguard to a fundamental freedom.

## V. Conclusion

[39] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data CETS No.: 108, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=12&DF=25/01/2010&CL=ENG.
[40] Chapter II
[41] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG
[42] https://epic.org/privacy/intl/coeconvention/ROTENBERG_COE_Jan28.pdf
[43] http://thepublicvoice.org/madrid-declaration/

EPIC supports the Reform of the Data Protection Framework. The General Data Protection Regulation builds on the important foundation established by the EU Data Protection Directive and it will contribute to the strengthening of privacy protections around the world.

**References**


Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), E.C. COM (2012) final, (Jan. 25, 2012) http://ex.europa/eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

EPIC, "EU Data Protection Directive" http://epic.org/privacy/intl/eu_data_protection_directive.html

European Consumer Organization (BEUC) Position Paper: Proposal for a Regulation (July 27, 2012), https://epic.org/privacy/BEUC-Position-Paper.pdf

The Public Voice, "Madrid Privacy Declaration" (2009) http://thepublicvoice.org/madrid-declaration/

TACD Resolution: Consumer Privacy Rights (May 24, 2012), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=343&Itemid=40

TACD Letter to US Congress on Hearing: "Internet Privacy: The Impact and Burden of EU Regulation" (Sept. 14, 2011), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=329&Itemid=40

TACD Resolution: Behavioral Advertising (June 21, 2011), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=298&Itemid=40

TACD Resolution: Cloud Computing (June 21, 2011), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=296&Itemid=40

TACD Resolution: Core Consumer Protection Principles in Electronic Commerce (Sept. 1, 1999), http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=135&Itemid=40

The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 1-2 (2012) available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.