"Accession to Convention 108: Benefits and Commitments"

Marc Rotenberg, President
Electronic Privacy Information Center
Washington, DC

Convention 108: From a European Reality to Global Treaty
Strasbourg, France
17 June 2016

Ladies and Gentlemen, distinguished guests, and friends, thank you for the opportunity to speak with you today. I am grateful for the invitation to participate in this historic conference.

For those who may not know, EPIC is an independent, non-profit research organization, based in Washington, DC, established to focus public attention on emerging privacy and civil liberties issues.

Over the course of many years, we have worked together to strengthen data protection, to promote international legal frameworks, and to defend the fundamental freedoms that are the bedrock of Constitutional democracies.

But I do not believe there has been a moment where the particular urgency of establishing a comprehensive legal framework for privacy protection was more apparent. Even as we are meeting today, negotiators are rushing to make changes to a political agreement that will likely collapse upon judicial review.

The obvious question is what will follow the so-called "Privacy Shield." That is the starting point for my remarks.

Let us quickly review the events of the last few years to understand how we reached this point.

Recent Developments

It was a little more than three years ago that we learned the scope of NSA surveillance of Internet users around the world. This was not simply the old-fashioned tracking of diplomats and suspected spies but rather the widespread surveillance of whole populations, of individuals who were monitored simply because they could be monitored. Private communications, web site visits, cell phone locations all were gathered up by secret means and poured into the enormous data centers maintained by the US National Security Agency for future analysis.

The reaction was immediate and widespread. Rejecting the view that citizens must give up fundamental rights to ensure public safety, civil society organizations, legal

experts, and political leaders banded together to seek an end to the programs of mass surveillance.

In the United States, legislators of both parties worked to enact the USA Freedom Act, which ended the bulk collection of domestic telephone record information and established public representation before the Foreign Intelligence Surveillance Court.

The Freedom Act was an important step forward, but it was only a partial step. The Section 702 program, which permits the bulk collection of non-US persons and often times includes the records of U.S. persons, continued as did many of the identification, tracking, and monitoring programs of transportation, finance, and employment under the authority of the Departments of Homeland Security.

Citizens outside of the US also rightly called for greater accountability of their own domestic intelligence agencies. While the surveillance capabilities of the National Security Agency pose unique challenges to constitutional democracies, it would be a fatal blindness for those who cherish fundamental freedoms to ignore the surveillance activities of other intelligence agencies, many of which operate with even less oversight than the NSA.

Hearings took place before European Parliament, the German Parliament, and other national legislatures. In some countries, reforms were adopted. In others, ministers resigned. Cases were brought to the Court here in Strasbourg by NGOs objecting to the surveillance by the GCHQ. These are important reform measures and represent a broader effort to maintain accountability and transparency across all countries. Democratic governments owe Mr. Snowden their gratitude.

Then came the historic decision of the Court of Justice of the European Union in the Schrems case. To find a case of equal significance in the long history of data protection we would need to go back to the German Constitutional Court decision that announced in 1983 a fundamental right to "informational self-determination." That decision sent shock waves throughout privacy law, its most recent echo in Article 8 of the Charter of Fundamental Rights.

The recent decision in Schrems, like the early census decision, has established a new foundation for the modern right to privacy. It will be a new starting point for how we understand privacy as a fundamental right.

Status of Privacy Shield, the EU-US Data Transfer Arrangement

We understand that in two weeks the Article 31 Committee will decide whether to approve the Privacy Shield**.** Much has been said for and against the Privacy Shield and it is not my intent to replay that debate for you today. But one point remains clear: it is unlikely that this arrangement for transborder data flows will survive another trip to Luxembourg. Indeed, under the very clear direction of the Court of Justice in the original

decision, it is unlikely that the "Shield" will survive judicial review with any of the Data Protection Authorities or national courts to which it is now subject.

The legal objections will be found in the recent opinions of the Article 29 Working Party, the European Data Protection Supervisor, and the statements of the EU NGOs who represent those whose personal data risk will be put at risk under an arrangement without legal force. And while the case is made by some that the United States offers "essentially equivalent protection," a fundamental problem cannot be ignored: even Americans do not believe that the United States has adequate protection for the privacy of their personal information. A leading industry analyst reported just last week that 45% of consumers are more worried about their online privacy than one year ago and 74% have limited their online activity in the last year due to privacy concerns." Meanwhile section 702 authority remains in place and the NSA seeks to promote greater surveillance and profiling of individuals using the essential services of the modern age.

So, we can anticipate that the legal arguments and empirical evidence for a new robust framework for a legal protection will accumulate rapidly if the Article 31 Committee accepts the text of the Shield. Even the proponents quietly concede that there are too many weaknesses as measured against the Schrems decision.

But the issue of data protection resonates also in the United States as a fundamental rights concern for Americans.

Data Protection and the 2016 US Election

It is probably fair to say that data protection is "the most important least well understand issue" in the 2016 United States elections. Every voter in the United States with a mobile phone, or a credit card, or a medical history, or an Internet account is affected by the policies and practices of organizations that collect and use their personal information. Yet there is a hardly a word spoken by any of the candidates about the issue.

This is remarkable because American voters are routinely reminded of the vulnerability of their personal information.

- Universities tell former students that their educational records, including payment information and bank details, have been breached, and they must obtain "identity theft prevention" services to guard against future acts of identity theft and financial fraud.

- Banks inform account holders that credit card numbers have been compromised, accounts must be closed, and new accounts opened

- All of the major Internet firms, including most recently Twitter and Linkedin, report massive breaches of password files

There is hardly a major financial firm, health provider, or Internet providers that has not suffered a massive data breach in the last few years. The consequences are born only in part by the firm because, of course, it is the individual's personal information, their credit records, their health information, that has been breached.

Perhaps most remarkable, the US Office of Personnel Management, the central government agency tasked with the storage and management of personal information across the federal government, lost control of 21 million records of federal employees, their families, and friends. Included in the data breach were records containing more than 5 million unique biometric identifiers, and the contents of the sensitive SF 86, which is the form that must be completed to obtain sensitive jobs in the U.S. government.

We were particularly upset that data breach because just a few years earlier, in an amicus brief for the US Supreme Court, EPIC had urged a right of information privacy to specifically prevent government agencies from collecting sensitive personal information, such as the data in the SF-86 form, they could not protect. In that case, *NASA v. Nelson*, the agency defended its poor data protection practices and the Supreme Court chose not to extend the right of information privacy, assuming that the data would be protected under existing law.

Now all federal employees, including the members of the Supreme Court, their families and their staffs, live with the consequences of that decision.

Still, organizations make ever greater demands for personal details, storing ever more sensitive information -- the digital images of a passports, identity documents, and credit cards – in databases that are not adequately protected, thereby accelerating the risks they have created.

And yet governments are reluctant to view this as a fundamental rights issue or even a consumer protection issue. Consumers are told that "notice and choice" is an effective privacy approach, and when there is a breach they will be "notified of the problem." Some US companies are before the US Supreme Court, actively seeking to overturn good privacy laws enacted by the US Congress over many years that would help reduce the risk of data breach and identity.

This is a course that will not end well for consumers or businesses.

In the United States, EPIC has launched a new nonpartisan campaign to promote Data Protection in the 2016 election. We have already spoken with leaders of the Republican party and they agree that "data protection" is a key concern for American votes. They point to their own recent efforts in Congress to update the Electronic Communications Privacy Act, as well as Privacy Enhancing Techniques, adopted in law, to protect personal identifiers when web log are transferred from private companies to government agencies under the recently adopted Cybersecurity Information Sharing Act.

We will next make recommendations to Democratic leaders next and then we will continue to promote data protection throughout the political season.

You can read more about the Data Protection campaign online. We have set out a brief "privacy platform" and included questions for the candidates. Through this campaign we hope not only to remind Americans that there are significant privacy problems but also that there are meaningful solutions to pursue.

We have highlighted several key goals for privacy reforms in the United States, including:

- Strong encryption
- Comprehensive privacy legislation based on Fair Information Practices
- New privacy laws to limits activities such as surveillance by drones
- Creation of a new federal privacy agency

We have specifically identified ratification of the Council of Europe Privacy Convention as one of the issues we believe candidates running for office in the United States should endorse.

Support for US Accession

Against this backdrop the case for US accession to Council of European Privacy Convention is clear, well established, and made repeatedly by civil society, technical experts, and legal scholars in the United States and around the world.

In 2009, more than 100 civil society organizations and privacy experts endorsed the Madrid Declaration. The Madrid Privacy Declaration reaffirms support for international instruments for privacy protection, such as Convention 108, identifies new challenges and calls for concrete action.

The Madrid Declaration specifically urges those countries that have not yet ratified Convention 108 together with the Protocol of 2001 to do so as expeditiously as possible.

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.

Even as discussion about new legal instruments moves forward, it is critical that not lose sight of the daily challenges that new technologies, new business practices, and new government initiatives pose.

Following the Madrid Declaration, in 2010 members of the EPIC Advisory Board, legal scholars and technical experts, urged then Secretary of State Hilary Clinton to seek US ratification of the COE Privacy Convention. We expressed our support for Secretary Clinton's remark on Internet Freedom and we commended her for stressing the importance of freedom of expression and privacy protection as fundamental rights in our digital age

We noted that many of the same concerns she expressed "animated the framers of the Council of Europe Convention who saw the promise of new technology but also recognized the risk to fundamental rights."

The United States should move to ratify the Council of Europe Convention on Privacy, the most widely known international framework for privacy protection. Some may object to the US supporting a Council of Europe convention, but it was only a few years ago that that the US rallied its European allies behind the COE Cyber Crime Convention, an international treaty that the US strongly supported.

Past as Prologue

Five years ago I had the honor speak with you on the occasion of 28 January, the day that marks the date that Convention 108 was open for signature

EPIC will continue our efforts to promote the Council of Europe Convention. The Convention is not a theoretical construct or a relic from an earlier era. It is a reminder of the centrality of privacy in our modern age, and the need to support and maintain international legal frameworks that enable growth and innovation, while safeguarding fundamental freedoms.

Thank you for your attention.

References

Anita Allen and Marc Rotenberg, PRIVACY LAW AND SOCIETY (West 2016), related resources *available at* www.privacylawandsociety.org

Article 29 Working Party, Opinion on Privacy Shield (April 13, 2016), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

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

Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," (January 21, 2010), *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm

EDPS, "Opinion on the EU-U.S. Privacy Shield draft adequacy decision" (May 30, 2016), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf

EPIC, "Data Protection 2016," *available at* www.dataprotection2016.org

EPIC, Council of Europe Privacy Convention, *available at* https://epic.org/privacy/intl/coeconvention/

EPIC, Letter of Legal Scholars and Technology Experts to Secretary of State Hilary Clinton (January 28, 2010)(regarding US Ratification of COE Convention 108), *available at* https://epic.org/privacy/intl/EPIC_Clinton_ltr_1-10.pdf

The Madrid Privacy Declaration, adopted November 3, 2009, *available at* http://www.thepublicvoice.org/madrid-declaration/

NGO letter to Commissioner Jourova and Secretary Pritzker to oppose a Safe Harbor 2.0 (November 13, 2015), *available at* http://thepublicvoice.org/EU-US-NGO-letter-Safe-Harbor-11-15.pdf

Marc Rotenberg, "On International Privacy: A Path Forward for the US and Europe," 35 *Harvard Internation Review* (Spring 2014), *available at* http://hir.harvard.edu/on-international-privacy-a-path-forward-for-the-us-and-europe/

Transatlantic Consumer Dialogue, Resolution on Privacy Shield (April 7, 2016), *available at* http://tacd.org/wp-content/uploads/2016/04/TACD-Resolution_Privacy-Shield_April161.pdf