

**Board Member Beth A. Williams**  
**“International Cooperation for Data Governance”**  
Privacy Symposium  
Venice, Italy  
April 21, 2026

Thank you so much for inviting me to participate in this esteemed gathering. I have been overwhelmed by the friendly welcome I have received from you all, my international colleagues, and I look forward to our exchanges today.

Visiting this historic city I have been reminded of the words of U.S. Secretary of State Rubio. In his speech at the Munich Security Conference earlier this year, he said,

It was here in Europe where the ideas that planted the seeds of liberty that changed the world were born. It was...Europe...which gave the world the rule of law, the universities, and the scientific revolution. It was this continent that produced the genius of Mozart and Beethoven, of Dante and Shakespeare, of Michelangelo and Da Vinci, of the Beatles and the Rolling Stones. And this is the place where the vaulted ceilings of the Sistine Chapel and the towering spires of the great cathedral in Cologne, they testify not just to the greatness of our past or to a faith in God that inspired these marvels. They foreshadow the wonders that await us in our future. But only if we are unapologetic in our heritage and proud of this common inheritance can we together begin the work of envisioning and shaping our economic and our political future.

This “common inheritance” is what I would like to speak about today.

This year, we are celebrating the 250<sup>th</sup> anniversary of the birth of the United States. Two hundred and fifty years may be a trifle in European terms, but it’s a big deal to us.

In 1776, Thomas Jefferson put to paper our founding principles: “We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.”

These principles were then echoed in our Constitution, which aimed to meld together thirteen different and headstrong colonies into one nation. Our founders started with the purpose of the document: "We the People of the United States, in Order to form a more perfect Union, establish Justice, ensure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."

We place the men who wrote these words on pedestals. But the values they championed were not born in 1776. America’s founders, as you all know, were inspired by great European thinkers – John Locke’s *Second Treatise on Government*, Montesquieu’s *Spirit of the Laws*, classical Greek and Roman ideas of civic virtue, and many others.

Our nations, and those that have adopted democracy across the world, possess this common inheritance. We value individual rights, due process, respect for human life, the right of the people to choose their leaders freely, and equality before the law. These are what we share.

But we are in a time of great technological change. The most vital question for us now is how to preserve our common values while embracing such monumental and rapid development.

Times like these are hard for those of us who are conservative—politically or dispositionally. As noted American writer William F. Buckley put it, our lot is to “stand athwart History, yelling Stop.”

But such futility is obvious. And it is more productive—and perhaps also more comforting—to remember that we have seen great change before, and endured.

\*\*\*

This symposium focuses on technological change, and in particular, the development of Artificial Intelligence. This new frontier portends change in the way we live our lives, conduct our work, and interact with each other. Its great promises are, not unreasonably, matched with great risks.

The challenge that faces us is not to crouch in fear, but to re-commit to our shared values, proudly. We must be the ones driving the technology to our common principles, the values that we know to be true because we were endowed with them by our Creator.

How to ensure this new technology strengthens our shared humanity, reflects our values, and supports our democracies is a task that many of us in this room face. We must do it together.

We already have significant examples of how these shared values are found in the seminal data privacy frameworks both in the United States and internationally. In the United States, the Fair Information Practice Principles (FIPPs) have guided government and private sector privacy policy for more than 50 years. And they formed the basis for U.S. contributions to the development of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, issued by the Organization for Economic Co-operation and Development, and the Asia-Pacific Economic Cooperation (APEC) Data Privacy Framework. And those principles are, in substance, similar to those of the EU’s GDPR. It was for those reasons that the OECD countries were able to agree in 2022 on the Declaration on Government Access to Personal Data Held by Private Sector Entities. In fact, the Declaration specifically cites, the “shared commitment to upholding democracy and the rule of law [and] ... protecting privacy and other human rights and freedoms.”

And it was shared values that enabled the U.S. government and the European Commission to create the Data Privacy Framework (DPF) that has enabled the continued transborder data flows between the United States and other countries. As you are probably aware, my agency, the Privacy and Civil Liberties Oversight Board (PCLOB), serves a role in reviewing the implementation of that agreement. Let me give you some background on PCLOB and then I will return to the DPF.

PCLOB was established at the recommendation of the bi-partisan commission that investigated the September 11, 2001 terrorist attacks, commonly called the 9-11 Commission. The Commission had argued for a number of increases in U.S. government power to combat terrorism, but then also wisely called for the establishment of a body to make sure those increases were balanced with proper respect for privacy and civil liberties. The balance there is key. Just like the previously mentioned privacy principles seek to balance individual rights with the legitimate need of governments to collect and analyze data, PCLOB's mission involves evaluating the national security value of specific counterterrorism programs and recommending ways to minimize their risks to privacy and civil liberties. This balancing is how the Board promotes public trust in the government institutions and processes that collect and use information, both domestically and for our international partners, as well, for example through the Data Privacy Framework.

PCLOB has been very productive in the last year—in fact, it's been our most productive year in the history of the agency. Since May of 2025, we have published four reports: on the Transportation Security Administration's use of facial recognition technology; on the U.S. government's implementation of Executive Order 14086, which implemented parts of the Data Privacy Framework; on the Federal Bureau of Investigation's use of open-source information; and on the amendments to the Foreign Intelligence Surveillance Act Section 702 program over the last two-and-a-half years.

I am proud to say that the hard work of our staff has been well-received. The reports have been praised for their contributions to transparency and public understanding of government programs. All the reports are available on our website, as well as other recent ones on the Terrorist Watchlist, Foreign Racially and Ethnically Motivated Violent Extremism, and the National Counterterrorism Center. And we have on-going investigations into aspects of the government's efforts to counter domestic terrorism, and the U.S. government's redress process under the DPF. As an individual member, I am also working to investigate government practices that may have encouraged the de-banking practices of individuals.

That leads me back to the Data Privacy Framework as another example of the partnership between the United States and our international allies based on common values. The DPF is implemented in U.S. law through Executive Order 14086, which is entitled, *Enhancing Safeguards for United States Signals Intelligence*. This Executive Order established government-wide safeguards for US signals intelligence activities consistent with the protection of privacy and civil liberties for all persons, regardless of nationality or place of residence.

PCLOB published a report in September of last year reviewing the implementation of updated policies and procedures adopted by the Intelligence Community. The report concluded that all intelligence agencies successfully updated their policies and procedures to comply with the order. Further, the report found that all Intelligence Community elements align the rules for the handling of non-U.S. persons' personal information collected through signals intelligence with the rules for handling of U.S. persons' personal information collected through signals intelligence activities. The U.S. government has also established a redress process and encouraged PCLOB to conduct an annual review of the processing of qualifying complaints.

PCLOB's staff is reviewing the redress mechanism now and how it operated with the first complaint that was received. We anticipate issuing a public report later this year.

In sum, PCLOB has played, and I expect, will continue to play an important role in the promotion of common values that enable international cooperation in data protection.

\*\*\*

As I mentioned earlier, PCLOB is also investigating how the government's efforts to counter domestic terrorism may have impacted free speech. Specifically, we are examining how the U.S. government was previously identifying and seeking to suppress what it deemed to be mis- and disinformation. The current Trump Administration reversed that policy through an Executive Order.

Only four years ago, in 2022, the U.S. Government's National Security Strategy stated that "the crisis of disinformation and misinformation, often channeled through social and other media platforms" was one of "the long-term contributors to domestic violent extremist threats."

So far, we have been unable to find that there was a basis for the assertions about a "crisis" of misinformation and disinformation driving domestic terrorism. The government certainly never released an analysis documenting one.

And yet the government took concrete steps to counter this speech, including the expenditure of large amounts of taxpayer money, and pressure campaigns to censor or suppress disfavored views.

This has been chilling to those who care about privacy and civil liberties. Free speech is sacred in the United States. It is the very first amendment in the Bill of Rights to our Constitution.

We are taught in school, "I may not agree with what you say, but I will defend to the death your right to say it." As Americans, we often attribute that quote to the American Revolutionary, Patrick Henry. But the phrase, of course, was written by an English woman, Evelyn Beatrice Hall, to describe the beliefs of a Frenchman, Voltaire.

Our nations have shared this value of free expression, and we must not let our fear—whether it be of actual harm or technological change—displace it. Silencing those with whom we disagree is the sure path toward becoming our own enemies.

I am hopeful that we can work together to safeguard the values on which our representative governments are built.

\*\*\*

Again, I am so grateful to all of you for this kind invitation to speak here today. I wish you the best, and I look forward to working together. Thank you.