STATEMENT OF

MORTON H HALPERIN

Before the

BUNDESTAG 1ST COMMITTEE OF INQUIRY

SEPTEMBER 8TH 2016

BERLIN, GERMANY

Members of the Committee,

It is an honor and privilege for me to appear before you to present my views on how to better protect the security of the United States and Germany and other like-minded countries as well as the privacy of the citizens and residents of their countries.

I have been engaged in issues at the intersection of national security and civil liberties since the early 1970s. For 18 years I directed the American Civil Liberties Union's project on national security and civil liberties, during which time I played a key role addressing many surveillance questions, including issues surrounding enactment of the Foreign Intelligence Surveillance Act (FISA), which required warrants for electronic surveillance for intelligence purposes in the United States.. Many years later, while working for the Open Society Foundations, I was engaged in the public debate on the FISA amendments Act of 2008 and other surveillance matters. I have testified before Congressional Committees on these issues on many occasions and welcome this opportunity to appear before this committee.

My professional engagement on these issues has, I am sure, been shaped by my personal experience of the impact of government surveillance that is not constrained by fundamental privacy principles. Beginning in May 1969 and continuing for 21 months, my family and I were the subject of a warrantless wiretap by the Federal Bureau of Investigation at the request of the Nixon White House. We filed a lawsuit against the responsible government offices, which led to a judicial ruling that such surveillance violated the American constitution.

While a court validated our claim that our fundamental rights were violated by the warrantless wiretap, most of my work on national security and civil liberties has focused on questions of how to balance legitimate national security concerns with fundamental civil liberties. In addressing these issues, my focus and that of almost everyone involved in these issues in the United States was, until recently, to develop solutions that simultaneously protect American security and the privacy rights of American citizens, wherever they might be, and of others persons in the United States.

Revelations by Edward Snowden in 2013, which included disturbing information about extensive U.S. surveillance of citizens of *other* countries, broadened the focus of concern. Since then privacy advocates have focused not only on surveillance of Americans by the US National Security Agency, or NSA, but also its surveillance of other private persons outside of the United States.

Even as we came to appreciate the need to broaden the scope of our efforts beyond the impact of US surveillance on US citizens, we have also come to understand that non-American intelligence services have conducted surveillance of private citizens of their own as well as other countries and maintain and use personal information about them, including sharing the information with the intelligence agencies of the U.S. and other governments. It is now clear that reform efforts needed to address the practices of all governments.

(Before I elaborate, I want to acknowledge that private citizens also need, as recent events underscore, the help of their governments in preventing intrusions into their privacy by private persons and hostile governments. The disclosures also called attention to the fact that governments spy on each other. These are two equally important and urgent matters, but beyond the scope of my testimony.)

The task today is to protect the privacy rights of individuals whatever their citizenship and location while enabling governments to gather, in accordance with rights respecting procedurs, the information they legitimately need to protect against terrorism and other threats to the security of their citizens.

In 2014, The President of the United States has taken an important step in the right direction by, for the first time, directing American intelligence agencies to take account of the privacy interests of private persons who are neither American citizens nor present in the United States. The President has placed some very modest limits on the collection of intelligence information, placed some limits on the use of information collected in bulk and directed the intelligence agencies to establish procedures to safeguard the person information of all private persons and directing that "to the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality." (Presidential Policy Directive/PPD-28, Signals Intelligence Activities, January 17, 2014)

This is only a first step and the reform embodied in this presidential directive needs to be strengthened and translated into enforceable legislation with effective oversight. Even so, the PPD takes an important first step by acknowledging the privacy interests of citizens of other countries. I am not aware of any other country publicly stating an intention to limit in any way the surveillance of, nor the storage or use of information concerning, persons who are neither citizens nor on their territory.

I would urge Germany to make such a commitment, but I would also urge it to do more: Germany is in a position to provide leadership in developing a wider framework of protection of individuals from unwarranted surveillance by foreign states. It can do so by expressing its willingness to work with the United States and other governments to enact appropriate reforms

that build on acknowledgment of the privacy rights of all private persons, whatever their citizenship and wherever they live.]

I believe that the most effective path for developing such a framework is by a group of like-minded democratic states—states with a deep commitment to privacy and other fundamental human rights—working together to develop common standards and procedures to govern electronic surveillance for intelligence purposes by any participating government directed at private citizens of other participating countries and individuals who are present on their territories.(I will refer to this group of people as "Protected Persons). The standards and procedures should also dealing with the retention and use of personal information about such persons however collected including procedures to identify the information which is entitled to protection.

While details would, of course, need to be fleshed out, let me offer a notional plan for how the United States and the Federal Republic of Germany might cooperate to bring this about.

A logical first step would be for the two governments to jointly announce their commitment to this principle of reciprocity and to the need to develop in a transparent way the agreed rules which would govern electronic surveillance of Protected Persons by a group of likeminded democratic countries. The two governments could then issue an invitation to other democratic countries, committed to the rule of law and with an independent judiciary, to join in negotiations leading to joint procedures.

Next, the governments that express interest should convene a multilateral negotiating process. The process should also, to the extent possible, be multi-stakeholder. That is, in addition to governments, companies that transmit and store this data should be included along with civil society organizations with expertise on surveillance and privacy issues.

The outcome of the negotiations should be a set of principles on surveillance of Protected Persons which each participating government would agree to implement according to its own legal procedures. A technical body might be created by agreement which would certify a country to have adopted the necessary legal structure and hence be entitled to the reciprocal protection of its citizens. States would, of course, be free to enact more stringent limits or to apply the agreed limits to all private persons, including citizens of other countries not party to the agreement, either as a matter of discretion or because they have determined that their domestic laws or international commitments required them to.

Here is are some tentative thoughts about what the agreement should cover and should require:

1. Surveillance of Protected Persons and retention and use of information about such persons may be conducted only consistent with international legal obligations and only if authorized by a duly enacted law which states clearly and publicly the authorities granted to intelligence agencies to conduct such surveillance.
2. Surveillance of Protected Persons for Intelligence purposes shall be limited to a specific set of publicly listed threats to be agreed by the participating governments and enacted by each state into law. (A good starting point for such a list is the one in PPD-28 for which

some bulk collection is permitted. These are espionage, terrorism, proliferation of weapons of mass destruction, cybersecurity threats, threats to military forces, and transnational crimes.)

3. Surveillance of a protected person would be defined as targeting a specific person's communications or searching for such communications in a larger collection of data whether collected by "bulk" collection or other means and even if lawfully collected. It would include collection of meta-data as well as the content of communications. The standard for collection (eg. Reasonable suspicion or probable cause) would need to be specified for each category of surveillance and might be different. For example, access to meta-data might require only reasonable suspicion and not probable cause.
4. Standards for retention and use of personal data of Protected Persons would also be specified. They would require that the same standards apply to Protected Persons as to citizens.
5. There would need to be a presumption that personal information would be treated as if from a Protected Person unless there was a reasonable basis to conclude that the person was a government official or not a citizen of any of the states which were party to the agreement and not on the territory of any of them. States may decide to simply apply these protections to all private persons as PPD-28 seeks to do.
6. Each participating state shall establish, consistent with its own laws and traditions, effective over-sight of the agreed standards and procedures. Such mechanism might include prior or subsequent judicial review, legislative oversight, and administrative oversight by bodies such as an Ombudsman. The technical evaluation body shall determine whether in each case the mechanisms are sufficient to insure compliance.
7. Each participating state shall establish a mechanism to permit any Protected Person to seek judicial relief if they reasonably fear that they have been subject to surveillance or data retention or use which violates the agreement guidelines. Again, the technical body would certify the adequacy of the procedures.

In the inter-connected world in which we live, only a mechanism adhered to by a large number of democratic states can give their citizens and residents assurance that their privacy is being respected. Such a structure would enable citizens and residents of these countries to make choices about what companies to entrust their data to without fear that it would have less protection if it is stored in or passes through one country or another that was a party to the agreement. It would remove a concern that could over time have a devastating impact on our ability both to have our privacy protected and to make genuine choices about how our data is stored and transmitted.

(Let me repeat, that citizens of democratic states, will also need help from our governments, as we are now learning, to protect our privacy from private predators and governments whose word cannot be trusted and who we would not trust to participate faithfully in this arrangement.)

Members of the committee, I hope my testimony will be useful and I would be pleased to answer your questions. Thank you.