A. What Is This Book About?

The globalized world requires the free flow of digital information. The commercial world requires this information to flow so it can operate in markets around the world. Governments require sharing of information to allow the efficient movement of people across borders and to provide safety, security, and benefits to individuals.

Modern globalization was brought about in large measure in the 1970s with the development of digital information processing. Digital information technology has enabled vast quantities of data to be stored, replicated, transmitted, and shared within seconds across national boundaries among individuals, organizations, and governments. The U.S. Government has a duty to protect its citizens, residents, and visitors. Likewise, sovereign democratic countries have the same duties toward their citizens, residents, and visitors. At the same time, governments often need to share personal information for purposes of security, law enforcement, and the issuance of benefits to their citizens.

When personal data is shared across national boundaries, what laws apply? The laws of the sending jurisdiction, the receiving jurisdiction, or, perhaps, through a negotiated agreement? The sender may effectively lose control over the information. For example, how would a sender of personal information prevent unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data that is in the control of a recipient in another jurisdiction? If the sender and recipient are independent sovereign states, how would one state assert some control over the other? Restrictions on these flows could cause serious disruption to the free flow of people, goods, and ideas; the effective
enforcement of laws; and the ability to provide benefits to individuals. To resolve these uncertainties, governments enter into information-sharing agreements.

The U.S. Government is party to dozens of government-to-government (G2G) information-sharing agreements on a spectrum of topics, including taxes, pension payments, securities enforcement, airline passenger data, lost or stolen travel documents, and law enforcement.

This guide is intended to be a reference tool on U.S. Government practice in G2G sharing arrangements. The U.S. Government’s practice in the area of cross-border information sharing covers dozens of agreements. This book will examine those agreements as a way of establishing how practice has evolved. In addition to reviewing past agreements, international privacy principles of Organisation for Economic Co-operation and Development (OECD) and Asian-Pacific Economic Cooperation (APEC) will be reviewed for their relevance to G2G sharing.

B. Who Should Use This Book?

This book is intended for lawyers, privacy professionals, and individuals who wish to understand U.S. practice for sharing personal information across borders. Particular groups that will find the Guide valuable are:

- Government practitioners engaged in personal information-sharing agreements;
- Homeland Security and law enforcement professionals;
- Practicing attorneys who have clients that may be affected by the sharing of their information between governments;
- Privacy professionals; and
- Individuals who may be affected by the sharing of their information with a foreign government and wish to understand their opportunities for access and redress.

C. The Political and Legal Context

The framework for the U.S. sharing of personal information is a combination of law, foreign policy, national security, economics, and privacy policy. While the United States has engaged in personal information sharing for decades, the number of factors influencing this sharing has grown. The Social Security “Totalization Agreements,” first signed in the 1970s, reflected the increased mobility of individuals to work and live outside their home countries and the need for governments to provide appropriate benefits. Since September 11, 2001, however, law enforcement and public safety concerns have led to an increase in the number of personal information-sharing agreements. In fact, the 9/11 Commission recognized the critical role information sharing plays in combating terrorism when it recommended that:
The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation.

This led the U.S. Government to enact a series of mandates to share personally identifiable information (PII) with its allies and friends.1 Many of the resulting agreements are collected here.

D. Foreign Policy and National Security Considerations

U.S. Government decisions to engage in information sharing are also influenced by more than data privacy frameworks. Information-sharing partners are also determined by foreign policy, national security, commercial, and immigration considerations. As foreign policy matter, U.S. leadership may look at whether the foreign partner is a close ally and whether it will serve our strategic interest. Such evaluations are likely to involve the Department of State. Other factors likely to be reviewed are the foreign partner’s respect for the rule of law, an existing framework of privacy laws, and the foreign partner’s record of trustworthiness.

National security considerations are noted by the 9/11 Commission report—that the United States should share information to better identify threats to our country. For example, U.S. immigration criteria for countries to participate in the Visa Waiver Program (VWP) were strengthened. Among added criteria was a law requiring that participating VWP countries enter into passenger information-sharing agreements.2

E. As a General Reference

Negotiating an international agreement is a specialty in itself.3 Negotiating personal information-sharing agreements is a growing specialty among agencies that requires a background in privacy, international affairs, and experience in the particular subject matter areas, such as consular law, criminal law, and/or immigration law.

---

1. Examples include the secretary of state’s authorization under the USA PATRIOT Act of 2001 to make agreements with foreign governments to share information from the visa lookout database for the purpose of fighting terrorism; Homeland Security Presidential Directive 6 (HSPD-6) that tasked the secretary of state to seek ways to access terrorist biographic screening information from foreign partners.


The U.S. Government agreements in the appendices should prove a useful reference for understanding the government’s practice in this area. While not exhaustive, the references included are examples of significant agreements. In addition, the appendices provide a collection of cross-border information-sharing guidelines such as OECD and APEC. All agreements and sources are public and footnoted for further reference.

F. A Note about Sources

All sources in this book are public. Many come from a particular agency’s website. An excellence source for researching specific agreements is the Department of State’s Office of the Assistant Legal Adviser for Treaty Affairs, which serves as the principal U.S. repository for U.S. treaties and other international agreements. Many of the agreements found in the appendices can be found at the Treaty Office’s online database.4