

## The Value of Understanding International Encryption Regulation

Encryption technology offers both substantial benefits (by protecting the confidentiality, authenticity, and integrity of business and personal information) and substantial risks (by making it easier for criminals and terrorists to conceal communications regarding illegal behavior). While most countries recognize the benefits of encryption, the associated risks have led many governments to impose controls on the import, sale, use, and/or export of encryption software, hardware and technical information. Companies that operate in a multinational environment can pay a significant price if they are not familiar with these controls.

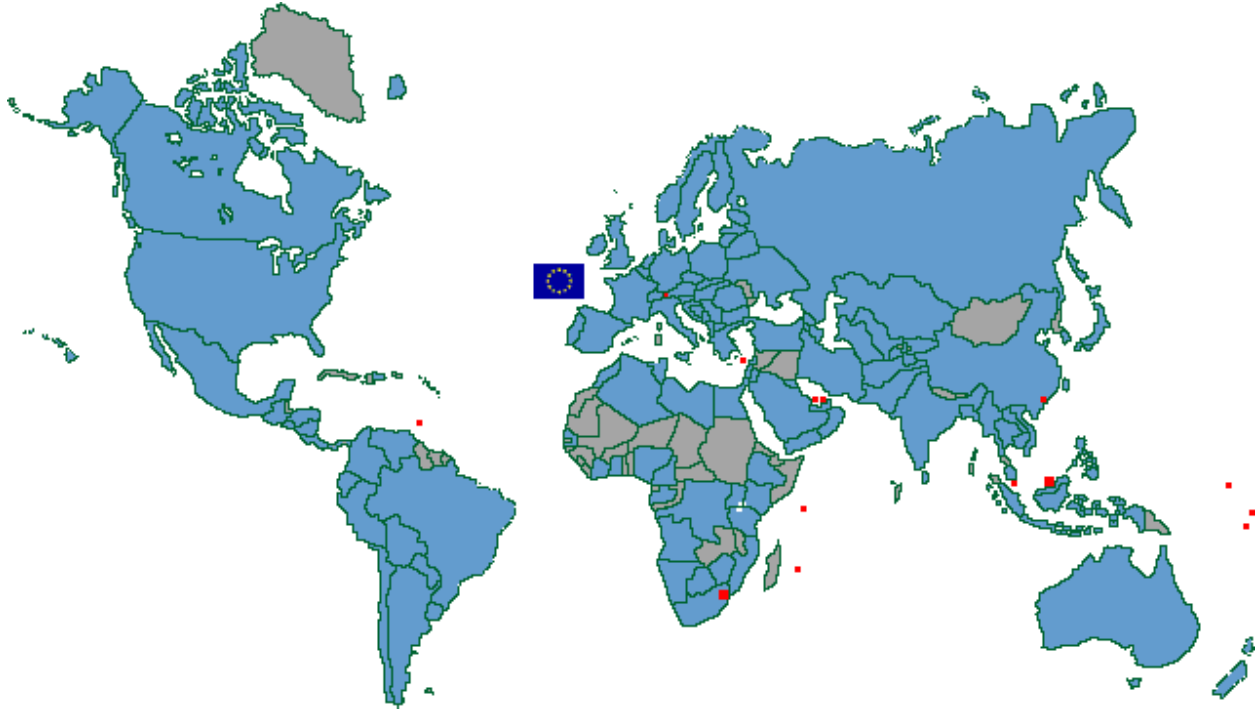
For instance, in the United States encryption controls cover export, but not import, domestic sale, or use, of encryption products. A violation of regulations related to the export of encryption may be punishable by civil monetary penalties, denial of export privileges, and criminal fines. US law may be violated not only if a US-origin product is exported from the United States without authorization, but also if it is “re-exported” from another country to a third country.

Outside the United States, numerous governments restrict the import, use, sale, and/or export of encryption. Some countries impose severe sanctions for a violation of their restrictions. Others use informal sanctions to address perceived misuse of encryption technology. In other instances, governments have blocked communications or confiscated encryption hardware or software. Finally, many companies have encountered substantial delays or the inability to deploy or sell encryption products in countries with established control regimes—typically because of a lack of familiarity with recent changes in local regulations and procedures.

An accurate understanding of international encryption regulation can help a company avoid costs and delays. Understanding the relevant laws and regulations also substantially reduces the risk of unintentional violations. In addition, an appreciation of the application and approval processes can allow companies to plan ahead on a global basis.

Steptoe’s subsidiary, InternatLaw L.L.C., offers a comprehensive, online guide to worldwide encryption regulations. The guide contains detailed reports on the encryption regulations of over 130 countries. Each report discusses applicable laws and regulations regarding the import, use, and export of encryption, including rules on “internal” corporate use, “intangible” imports and exports (i.e., Internet downloads or uploads), and temporary imports of encryption by business travelers on laptops or other mobile devices. Each report also covers applicable penalties and provides local points of contact for additional information. A list of countries currently covered by the guide follows.

# Scope of County-by-Country Guide to Encryption Regulation



Afghanistan	Croatia	Ireland	Nicaragua	Switzerland
Albania	Cyprus	Israel	Nigeria	Taiwan
Algeria	Czech Republic	Italy	Norway	Tajikistan
Angola	Denmark	Japan	Oman	Tanzania
Argentina	Dominican Republic	Jordan	Pakistan	Thailand
Armenia	Ecuador	Kazakhstan	Panama	Togo
Australia	Egypt	Kenya	Paraguay	Trinidad & Tobago
Austria	El Salvador	Kuwait	Peru	Tunisia
Azerbaijan	Estonia	Kyrgyzstan	Philippines	Turkey
Bahrain	Ethiopia	Laos	Poland	Turkmenistan
Bangladesh	European Union	Latvia	Portugal	Uganda
Belarus	Fiji	Lebanon	Qatar	Ukraine
Belgium	Finland	Libya	Romania	United Arab Emirates
Bolivia	France	Liechtenstein	Russia	United Kingdom
Bosnia and Herzegovina	Gabon	Lithuania	Samoa	United States of America
Botswana	Germany	Luxembourg	Saudi Arabia	Uruguay
Brazil	Georgia	Macedonia	Senegal	Uzbekistan
Brunei	Ghana	Malaysia	Serbia	Venezuela
Bulgaria	Greece	Marshall Islands	Seychelles	Vietnam
Cambodia	Guatemala	Mauritius	Singapore	Yemen
Cameroon	Honduras	Mexico	Slovakia	Zimbabwe
Canada	Hong Kong, S.A.R.	Montenegro	Slovenia	
Chile	Hungary	Morocco	South Africa	
China	Iceland	Mozambique	South Korea	
Colombia	India	Myanmar (Burma)	Spain	
Congo (Dem. Rep.)	Indonesia	Namibia	Sri Lanka	
Costa Rica	Iran	Netherlands	Swaziland	
Côte d'Ivoire	Iraq	New Zealand	Sweden	

For more information on the Guide, or to set up a demonstration, contact [Michael Vatis](#), telephone +1 212 506 3927, or [Sally Albertazzie](#), telephone +1 202 429 3062.

## Step toe's E-Commerce Practice Group

### Overview

Encryption regulatory issues have been, and will continue to be, a hazardous area for companies attempting to comply with varying regulations around the world. Steptoe & Johnson LLP's E-Commerce Practice Group offers a unique service to clients seeking to navigate worldwide cryptography regulations. We have an international team of lawyers based in both the United States and Europe, whose combined experience spans decades.

As well as being leaders in encryption issues, Steptoe has also developed a broad network of information sources around the world, including government agencies, multilateral organizations such as the OECD, local embassies, commercial networks and organizations, and local counsel. These contacts give us the unique ability to send quick inquiries to numerous countries and to obtain formal or informal guidance about encryption regulations. Our contacts are particularly useful in countries that do not publish the details of their encryption policies. With the help of our extended network, we provide both counseling on country-by-country requirements and assistance in obtaining import, export, sale, and/or use licenses around the world.

Step toe's E-Commerce Practice Group represents leading financial institutions, information and telecommunications services, hardware and software firms, and other multinational organizations on a wide array of issues concerning privacy, information security, and electronic commerce. This includes litigation, dealings with law enforcement or security agencies, regulatory compliance, internal investigations, and strategic planning.

**Michael Vatis** is a partner in Steptoe's New York office. His practice focuses on Internet, privacy, security, e-commerce, and technology matters, including issues involving security, intelligence, and law enforcement. He has extensive experience advising clients on US export controls on encryption as well as on foreign jurisdictions' laws governing the importation, sale, use, and export of encryption. He was the founding director of the National Infrastructure Protection Center at the FBI, the first government organization responsible for detecting, warning of, and responding to cyberattacks, including computer crimes, cyber terrorism, cyber espionage, and information warfare. He was also Associate Deputy Attorney General at the Department of Justice, where he helped oversee the Department's activities and policies in the areas of national security, counterterrorism, intelligence and counterintelligence, cybercrime, and encryption. Mr. Vatis has regularly testified before congressional committees on counterterrorism, intelligence, and cyber security issues. He is also interviewed on television, radio, and in print media, and has been a guest lecturer at law schools and universities and a frequent speaker at industry conferences worldwide.

**Stewart Baker** rejoined the firm as a partner in Steptoe's Washington, DC office following 3-1/2 years at the Department of Homeland Security as its first Assistant Secretary for Policy. Once described by The Washington Post as "one of the most techno-literate lawyers around," Mr. Baker's practice covers national security, electronic surveillance, law enforcement, export control encryption, and related technology issues. He has been a key advisor on US export controls and on foreign import controls on technology. He has also advised companies on the requirements imposed by the Committee on Foreign Investment in the United States. In addition, he was responsible for spearheading the government-private sector

## Step toe's E-Commerce Practice Group

coalition that permitted major telecommunications equipment manufacturers and carriers to break the decade-long deadlock with law enforcement on wiretapping of modern technology, permitting successful implementation of the Communications Assistance for Law Enforcement Act (CALEA).

**Alexandra Baj** is of counsel in Step toe's Washington office. Her practice focuses on export controls and economic sanctions laws and regulations, anti-corruption investigations and compliance, international trade, and security clearance issues. She is a key lawyer in Step toe's encryption practice, advising companies on encryption import, export, and use laws and regulations under US rules and in jurisdictions around the world. Her encryption practice also includes encryption and product classifications.

**Maury Shenk** is a Technology, Media & Telecommunications consultant and adviser to the London office of Step toe & Johnson and is a dual-qualified US/UK lawyer. He has extensive experience on regulatory, commercial, transactional and policy matters involving electronic commerce, representing many leading technology companies from the United States and Europe. He advises clients on the legal aspects of business on the Internet, including online agreements, data protection, information security, intellectual property and competition. Maury frequently handles technology transactions, including M&A and outsourcing agreements. He works with Step toe & Johnson's leading encryption export/import team, and is experienced in encryption licensing proceedings in the US, UK, France, Russia, China and other jurisdictions.

**Sally Albertazzie** is a specialist in Step toe's E-Commerce practice group. She has managed the Country-by-Country Guide to Encryption Regulations since its inception in 1999 and has worked with Step toe's "eTeam" for over 15 years on a wide range of high-tech issues, including encryption, data privacy, data security, and lawful intercepts. Ms. Albertazzie is a graduate of Georgetown University's Paralegal Institute.

The team has represented numerous companies providing encryption, telecommunications, information services, and electronic payment services on litigation, regulatory, legislative and corporate contractual matters. The team has also advised numerous firms on e-commerce, privacy, data protection, data retention, and consumer protection in the United States, European Union and other jurisdictions.

Our clients include some of the world's most prominent companies in a variety of business endeavors:

- Internet service providers
- Communications providers
- Voice over Internet Protocol providers
- Numerous software and hardware companies
- Global investment and commercial banks
- Energy companies
- Other technology companies