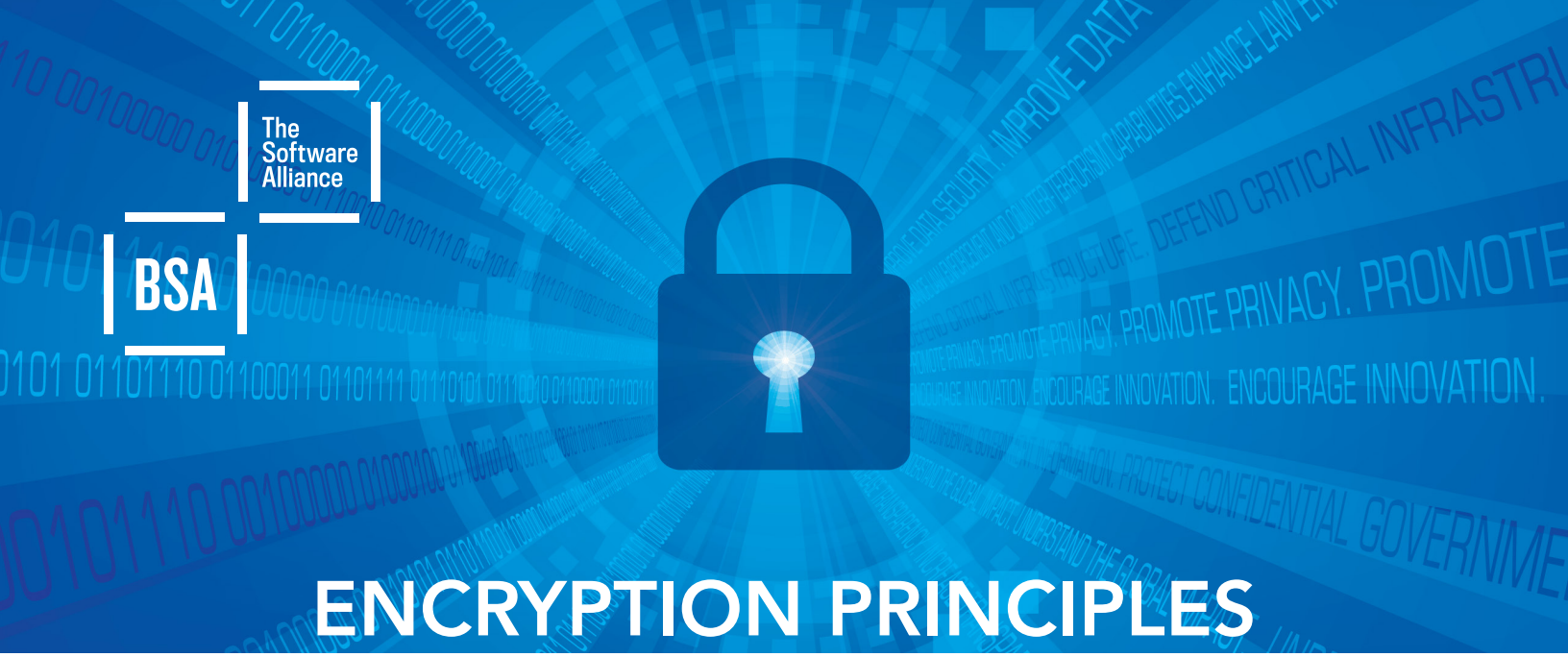

ENCRYPTION PRINCIPLES

A Comprehensive Approach to Promoting Global Cybersecurity, Public Safety, Personal Privacy & Prosperity

The current polarized debate on the use of encryption to promote security regrettably assumes that solutions must have winners and losers. We forcefully reject this assumption.

Effectively addressing all legitimate interests requires acknowledging two realities: first, increased reliance on secure information technologies improves our daily lives, advances our economy and individual freedoms; and, second, bad actors will misuse security tools to pursue their illicit aims — from terrorism and violent crime to cyberattacks.

These realities establish two goals, both of which must be achieved:

1. **Criminals and terrorists must be stopped, and**
2. **Individuals' security and privacy to enjoy and lead daily lives in the digital world must be safeguarded.**

An enduring solution to the encryption challenge must balance the legitimate rights, needs and responsibilities of:

» **Governments** to protect personal and confidential information they hold and to prevent terrorist and criminal acts and prosecute offenders;

» **Individual citizens'** right to secure the privacy of their personal information.

» **Providers of critical infrastructure and essential services** — including water, electricity, transportation, banking, and health — to protect their operations from cyberattacks;

» **Third-party stewards** of personal data and confidential business information to protect the data entrusted to them;

» **Innovators** to develop products and services that improve our daily lives and drive economic growth free of government mandates.

more >>

PRINCIPLES FOR ACTION

Moving the encryption debate forward will require many groups to come together to craft solutions. We will evaluate any proposed legislation, regulation or policy on encryption in light of the following principles:

1. **Improving data security:** Providers of data services — storing, managing or transmitting personal or business data — must be permitted to use the best available technology to thwart attacks against that data or the entities and individuals who depend on those services.

2. **Enhancing law enforcement and counter-terrorism capabilities:** Law enforcement agencies, subject to appropriate privacy and civil liberties safeguards, should have access to the best available resources, information, and tools available to prevent and prosecute terrorist and criminal acts.

3. **Promoting privacy:** Individuals have a right to be secure in their public, private and commercial lives and interactions.

4. **Protecting confidential government information:** National, state and local agencies should ensure that the data they hold is secure against threats of domestic and foreign intrusion.

5. **Encouraging innovation:** Developers and providers of innovative data security tools should be free of government mandates on how to design technology products and tools for digital security.

6. **Defending critical infrastructure:** Providers of essential services, such as banking, health, electricity, water and other critical infrastructure providers, should be empowered to provide the best available security technologies to their users. Best practices should be widely shared.

7. **Understanding the global impact:** Criminal and terrorist acts are not limited by national borders, and laws and policies must create consistency and clarity in all countries where security technologies are developed and used.

8. **Increasing transparency:** There should be full, transparent, and considered public dialogue before any legislative proposal concerning the future of technology mandates or encryption is adopted.