Decoding the encryption conversation

Brunswick's GEORGE LITTLE and SUSAN HO consider a valuable but contentious tool

Nearly 20 years ago, the "conflicting objectives" of data encryption were identified by the Brookings Institution, a US think tank, as: "civil liberties, economic competitiveness, law enforcement and national security."

These conflicting objectives continue to divide opinion, and encryption is hotly debated by a wide group that includes investors, journalists, governments, business leaders and consumers.

However, encryption's effectiveness as a cybersecurity tool is doubted by none. And a company's approach toward encryption can see them reap huge reputational benefits or, conversely, face reprisals from regulators, the media and consumers.

At its most basic, encryption makes data unintelligible without a "key" of some kind. Digitally encrypted data, for example, may appear as random symbols, letters or numbers. While encryption will not keep attackers from accessing your files it will prevent them from understanding the data. Encrypted hardware means that a lost cell phone or laptop does not necessarily compromise security.

As the distinction between data privacy and data security continues to be blurred, encryption has become almost synonymous with both. (See "Bridging the trust divide," Page 11, for Brunswick Insight's research on this trend.) The mathematics that underpin cryptography are incredibly sophisticated, but to many the encryption equation is fairly simple: it helps keep information secure and private.

Cybersecurity itself is a subject that more and more businesses are prepared to discuss with stakeholders, a conversation in which encryption plays a growing role. Companies that manage this discussion well differentiate themselves from competitors that choose to remain silent. At the same time, those who engage also build trust, communicating to their customers: we care about protecting your data as much as you do.

TECHNOLOGY COMPANIES have been at the forefront of this movement. This makes sense. Tech companies have both the necessary credibility and the incentives. The Information Technology and Innovation Foundation think tank estimates that Edward Snowden's leaks about the US National Security Agency surveillance wound up costing Silicon Valley up to $35 billion in annual revenue, as customers shunned the purchase of new products or equipment that could put their personal information at risk of surveillance.

2. THE KAMA SUTRA (LANGUAGE OF LOVE)

One wouldn't expect to encounter encryption in the Kama Sutra. The ancient instructional guide to the art of lovemaking was put together by Hindu philosopher Vatsyayana, believed to have lived around the 2nd century. One section of the book lists 64 arts that an ideal lover should master. Number 44 is *mlecchita vikalpa*, or "the art of understanding writing in cypher and the writing of words in a peculiar way." Presumably this technique allowed lovers to communicate in secret.

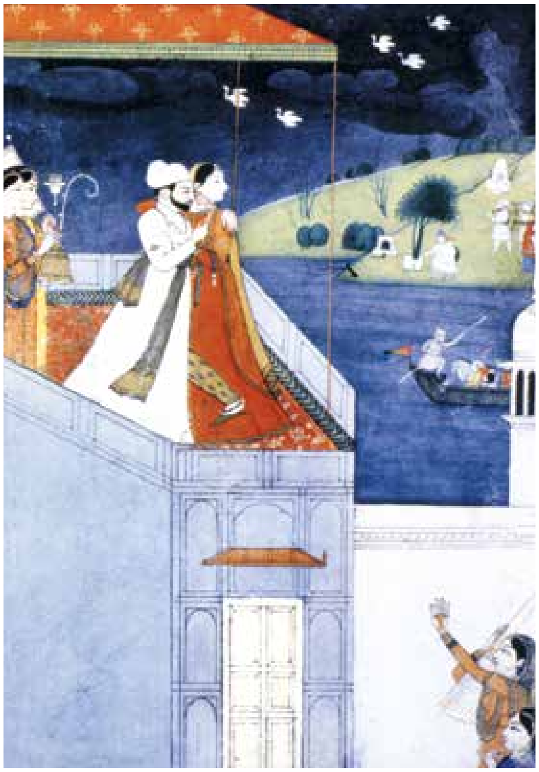

IMAGE: THE GRANGER COLLECTION, NEW YORK

WhatsApp, a mobile messaging application with more than 1 billion users, quietly enacted encryption in 2016. "Privacy and security is in our DNA," it said, "which is why we have end-to-end encryption in the latest versions of our app." The move, "ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp." The feature has been broadly welcomed by users, but it highlights the "conflicting objectives" that the Brookings Institution raised in 1997: some government bodies, increasingly concerned with terrorism and national security, are less enthusiastic (see below).

Telegram, a global messaging application with 100 million users, and Allo, Google's messaging service, have adopted similar encryption measures. The operating systems for both Android phones and iPhones have encryption features built in. Online file hosting services, such as Dropbox, encrypt data stored in the cloud. Microsoft's email service, Outlook, and its suite of Office365 products, are encrypted. All highlight encryption on their respective websites.

THE ENCRYPTION CONVERSATION is by no means restricted to Silicon Valley. Any industry or business that collects and needs to protect data can, and perhaps should, join in.

A 2014 survey conducted by the Pew Research Center found that only 26 percent of American adults trusted that companies with whom they did business would keep their records private and secure. Credit card companies, which scored highest on the survey, inspired confidence in only 38 percent of respondents.

SNAPSHOT GLOBAL SECURITY REGULATION

Even world powers that traditionally reside at opposite ends of the political spectrum tend to be reasonably aligned on the question of data privacy. In general, they want some form of access to encrypted data, citing it as an issue of national security. Many businesses oppose such an idea.

A bill has been introduced in the US that could force companies to decrypt and hand over data, though any progress on the issue is unlikely until after the presidential elections in November 2016. In the UK, the proposed Investigatory Powers Bill contains a similar provision.

Different versions of mandatory key disclosure legislation – as in handing over the key that decodes encrypted data – exist in countries such as Australia, China, France, India, Russia and South Africa.

But global laws on cybersecurity vary widely and extend far beyond data privacy and encryption. Many stipulate disclosure requirements and mandatory cybersecurity measures for businesses.

The EU is set to implement groundbreaking legislation that will come into effect across the continent by 2018. (See "Following the rules is not enough," Page 16, for a closer look at EU regulation.)

Hong Kong's Monetary Authority announced an initiative in May 2016 to improve cybersecurity among banks, the same month that a bulletin was issued by the local regulator to all licensed companies based in Hong Kong with suggestions on how to strengthen their cybersecurity.

In Singapore the Cybersecurity Act, set to be introduced in 2017, will empower the government to play a greater role in managing cyber incidents in the event of an attack on key companies or industries in the private sector.

> "While the regulatory landscape is far from straightforward, compliance alone should not be the goal"

Brazil enacted the Marco Civil da Internet in 2014, described as a civil rights framework for the internet, and this was reinforced by further regulatory legislation in 2016.

No unified legislation on data privacy exists in the Gulf Cooperation Council region, although the alleged 2016 security breach at Qatar National Bank, the largest lender in the Middle East and Africa by assets, has drawn attention to cybersecurity. Some GCC countries are beginning to write laws of their own. Qatar's cabinet approved a data privacy law in January 2016, while Dubai issued a law addressing cybersecurity in late 2015, although specific policies and an oversight authority to enforce them have yet to be implemented.

But while the regulatory landscape is far from straightforward, compliance alone should not be the goal. Companies that take the initiative and set their own standards for data privacy and security will earn trust from their stakeholders that will serve them well in the event of a cyber attack.

This at a time when customers are increasingly reluctant to give businesses either their data or their trust (see “Trust divide,” Page 11). Trust is in short supply and businesses are competing with each other to win it. As a 2015 *Harvard Business Review* article said, “In an information economy, access to data is critical, and consumer trust is the key that will unlock it.” This is the “data premium,” the value an organization gains from effectively communicating its careful stewardship of the precious data with which it is entrusted.

So why isn’t every company encrypting every byte of their data? To begin with, encryption costs money and takes time to implement. Often, it also comes at the expense of efficiency, a trade-off not all businesses are willing to make. End-to-end encrypted data can’t be easily monetized, shared or studied (See “Safety in numbers,” Page 21, on how companies are using their data to tackle social problems). And of course, not all information a company stores warrants such security.

Even if businesses do encrypt their data, they may not be interested in making that practice public. As we have seen, the conflicting objectives highlighted by Brookings remain contested.

In the wake of recent terrorist attacks, law enforcement agencies have said that encryption puts lives at risk by greatly limiting their ability to monitor and investigate dangerous criminals. Others have argued that providing any third-party access to encrypted data is prone to abuse and undermines the security of all information protected by similar encryption techniques.

This debate was inflamed after a terrorist attack at San Bernardino, California at the end of 2015. As part of its ensuing investigation, the FBI asked Apple to unlock an iPhone that belonged to Syed Farook, one of the alleged perpetrators. Apple offered to assist the FBI in other ways but didn’t create a code to unlock the phone, saying that doing so would jeopardize the security of all iPhones and set a dangerous legal precedent. The FBI eventually accessed the phone without Apple’s help, but both sides agree that the broader issues raised by the case remain unsettled.

THE PERCEPTIONS surrounding encryption, about what governments need to do – and should be able to do – in the name of national security, vary widely by culture and by country. This can make encryption a sensitive and complicated topic for businesses with a global presence to navigate.

Striking a balance in both tone and message is difficult, but critical. Businesses that broadcast the strength of their encryption could motivate an attacker to try to prove otherwise or, in certain countries, face a backlash, and perhaps legislation. Those that describe their “AES 256-bit-encrypted” hardware will be understood only by the most tech savvy, while companies that oversimplify the issue may have their competence called into question.

In such a delicate environment, businesses may be wary of saying anything at all. Talking about encryption can be contentious. But the bigger risk is to leave customers in the dark about what is being done to protect their data.

3. AL-KINDI (PATTERN RECOGNITION)

الجمهورية العربية السورية
SYRIA
THE 6TH CONFERENCE OF THE ARAB MINISTERS OF CULTURE
1987
POSTAGE
بريد
330

The 9th century Iraqi polymath Abu Yusuf Ya‘qub ibn Ishaq Al-Kindi, commonly known as Al-Kindi, pioneered frequency analysis, a powerful codebreaking technique. Certain letters and spelling constructions occur more often than others. A symbol that appears most often in a coded message is likely to correspond to the letter most commonly used in that language’s alphabet, and so on. Frequency analysis went on to be used to crack codes in many languages for centuries afterwards. Syria is one of many countries to release a postage stamp honoring Al-Kindi (left).

GEORGE LITTLE is a Partner in Brunswick’s Washington, DC office, specializing in crisis, cybersecurity, reputational and public affairs. **SUSAN HO** is Head of Brunswick’s Hong Kong office. She was formerly Global Head of Brand at Standard Chartered. Additional reporting by **SIOBHAN XIAOHUI ZHENG,** a Director in Hong Kong who specializes in cybersecurity.