Encryption, Lawful Access, and Back Doors

Written by Doug Lowry
President, Marpex Inc.

Two Perspectives:
1. Encryption and Lawful Access
2. Encryption and Back Doors

Legitimacy:
3. Enterprises and Need to Know
4. Law Enforcement, National Security and Need to Know

Security:
5. Blocking Irresponsible Invasion of Privacy
6. Maintaining Full Strength Encryption

Decision:
7. A Tale of Two Products

1. Encryption and Lawful Access -- A Perspective:

Lawful access is a phrase favored by the U.S. Department of Justice in its quest for strong encryption systems that provide for decryption of content in special circumstances. The norm in our society is respect for the privacy of every person. Attorney General William Barr puts that respect within this context:

> Enjoyment of all the personal rights we cherish – whether to life, liberty, property, speech, or privacy – ultimately depends upon our ability to maintain a safe society. Whether you agree with John Locke about everything, he was certainly right about that. The founding document of our republic, the Constitution, states at the outset that one of the principal reasons we have framed our body politic is to provide this security – "to provide for the Common Defense," that is, security from foreign enemies; and "to insure Domestic Tranquility," that is protection from the predators within our society. Unless society as a whole has the ability to preserve this peace and security, our rights ultimately become meaningless.

Privacy derives from the dignity of every person, a foundational value that is essential to human society. Security of the community is likewise a foundational value. Personal privacy and communal security are worthy priorities that co-exist in a dynamic balance. If that balance is lost, one or the other value is violated. In China, personal privacy of citizens is subordinated totally to stability of the

regime. In the United States, minimal defense of society (e.g., cameras that detect vehicles running red lights) may be decried as invasion of privacy.

Lawful access is an attempt at balance. Let there be privacy, except when a responsible judiciary finds cause to suspect terrorist or criminal intent.

2. Encryption and Back Doors -- A Perspective:

The NSA (a.k.a. "No Such Agency" in the 1990s) and the Clinton administration brought us the Clipper Chip imbroglio. This interesting bit of history put an entire industry up in arms so that the Clipper Chip sank quickly into political oblivion. But suspicion lingers on, decades later. The choice of terms says it all. *Back doors* in encryption? Bad, bad! *Lawful access*? Chill out, man, society is kept safe.

If users are unaware of a back door, or if there are not clear rule-based grounds on which content may be decrypted, or if there is not a culture of integrity among the people who are charged with security, then existence of a back door would lead sooner or later to disaster or at least to "interesting times".

An encryption back door is also illegitimate if the users regard the content as their own, unless they knowingly receive some quid pro quo (such as precision search) that they believe merits the sacrifice of their privacy.

Surveillance becomes increasingly unpopular as people learn of its misuse and overuse.

Government demands or pleas for lawful access are commonly resisted by the cybersecurity industry on the grounds that back doors would weaken encryption and drive citizens to get privacy software offshore. There is also resistance to administrative state attitudes which President Lincoln might have termed "people of the government, for the government, and by the government".

In sum, when we speak of encryption, whether in terms of back doors or lawful access, the main concerns relate to perceived legitimacy and to quality of security.

3. Enterprises and Need to Know -- Legitimacy:

Applications that feature encryption-with-a-back-door could be offered by email service providers, cloud storage firms, even government-approved entities. Is it legitimate for enterprises to require their members to use these products? For enterprise, read also *corporation*, *government department, association*, etc.

Consider the simplest ethical case. The underlying assumptions for an enterprise-based implementation are:

1. that corporate resources including files and messages processed on its computer equipment are owned by the enterprise;
2. that its leaders may require that high quality encryption be applied routinely to defend the enterprise's non-public information assets; and
3. that enterprise leaders may legitimately delegate authority to decrypt any of its information assets.

The case for legitimacy is stronger to the extent that all users are aware that the encryption system provides lawful access to corporate leaders to decrypt any files or messages that users have created on corporate equipment

4. Law Enforcement, National Security, and Need to Know -- Legitimacy:

Privacy of communications is an expectation born of American history. The Declaration of Independence was a call to revolution against "tyranny" and "despotism". Article II of the Constitution, the right to bear arms, is widely interpreted as a defense against government intrusion into the lives of a free citizenry.

It is in this context that law enforcement and national security personnel contend on behalf of public safety and security.

The problem at its roots is essentially one of political will. Congress responds to public opinion. But as citizens each of us is conflicted; our ideal would be privacy for ourselves and effective surveillance for bad guys. In reality, our view is influenced by the latest news cycle. Terrorist atrocity today? Our congressional rep will hear tomorrow that we want better security. Revelation of a previously unreported government surveillance mechanism? Our congressional rep will hear tomorrow that our privacy is not to be messed with. In this teeter-totter public opinion environment, our political leaders are charged to shape solid policy which will provide an effective ongoing balance between privacy and public safety needs.

Their task is not easy.

An irony: I write this paragraph on March 13, 2020. The public is clamoring for government action to protect our society in the face of the coronavirus pandemic. On this day, public security is at front of mind and urgently desired across the political spectrum.

5. Blocking Irresponsible Invasion of Privacy -- Security:

There are risks to enabling third-party access to encrypted content. Whether the third party offender is a senior officer in an enterprise, an Information Technology worker, or some nameless person deep within a government bureaucracy, things can go wrong and will go wrong. Data fishing expeditions, personal targeting, political mischief are intentional abuses of privacy. Fraudsters may pose as people authorized to request decryption of files and messages. Sheer incompetence of persons authorized to access encrypted content can lead to even worse outcomes.

To offset these risks, checks and balances must be built into the system. One method is to split resources so that no one person has the ability to "open the back door". In an enterprise, the cooperation of two or more persons should be required to invoke decryption of any file or message. At the national level, decryption requires a formal request by a security or police entity followed up by a court order. The political cost of bypassing these checks and balances is steep.

6. Maintaining Full Strength Encryption -- Security:

The cybersecurity industry concern over back doors is well grounded. If intended third parties can circumvent encryption, then hackers have a strong incentive to reverse engineer the software. Design of a competent encryption engine requires different thought processes than design of third party intrusion. Vulnerabilities may result from the attempt to dovetail lawful access capability into the system. Hackers would aim to discover both the method of lawful access *and* any vulnerabilities. If they succeed, hackers gain access to perhaps all of the documents that were encrypted by the many users of that particular encryption engine.

It's fruitless to advise programmers to never leave vulnerabilities. By all means try, but vulnerabilities will happen.

It's better to design the encryption algorithms together with the third party access as a single coherent unit.

- Design so that multiple resources must be obtained and hacked before a single encrypted document is put at risk.
- Design so that the user can remain blissfully ignorant of keys and key management.
- Design with the certainty that some users will "get cranial cramps" (do stupid things) that make them vulnerable to social engineering / deception.
- Design so that, should one user be compromised, there is the minimum possible cascading effect upon the work of other users.
- Design so that mission-critical resources are rarely (if ever) online.

The goal is to achieve maximum security for output of the encryption system, independent of whether it does or does not provide lawful access / a back door for authorized third parties.

7. Decision -- A Tale of Two Products:

Marpex Inc. presents two products, one without and the other with provision for lawful access.

MarpxPrivacy focuses on the right to privacy and offers lawful access only in the sense that a nation state likely has computing resources sufficient to decrypt a few selected files and messages, but at a cost that makes mass surveillance prohibitive.

Extreme Encryption™ is vastly stronger, but provides means for an enterprise to recover its own content *and* for the U.S. judiciary to determine when there is probable cause to authorize decryption of selected content in defense of communal security.

In the discussion that follows, let's use the word *confidants* for persons who exchange messages and files confidentially. In this context, a *roster* is a list of confidants.

Extreme Encryption™ shares basic methods with *MarpxPrivacy*. But the two products by Marpex Inc. are distinct in many ways.

Feature	Marpx Privacy	Extreme Encryption
Invisible key option	Yes	Yes
Private Exchange Tool (PET) files	No	Yes
Digits in count of unique keys	13	624
Resistance to brute force attack	High	Extreme
Roster	Visible	Invisible
Roster management responsibility	Self	Provider
Explicit lawful access feature	No	Yes
Quantum resistant feature	No	Yes
Distribution	Worldwide	United States
Set-up time and learning curve	Moderate	Negligible

The *MarpxPrivacy* program as described at https://Marpx.com offers excellent personal privacy and reasonable levels of security for organizations. A hacker using brute force at the rate of one unique key per second would need 111,000 years to break one message. Advantages of *MarpxPrivacy*: (a) It's free and available anywhere in the world. (b) The user has direct control of the roster, and

can at any time add new confidants. (c) Many would see *MarpxPrivacy*'s lack of a lawful access feature as a plus.

Extreme Encryption is simpler to learn and to use. In contrast to the free product, *Extreme Encryption* is vastly more secure; hacking by brute force attack is "computationally infeasible." There is an unthinkable number of keys to try. In the face of advances in quantum computing, *Extreme Encryption* strength can be readily scaled upward. This scalability makes the system impervious to hacking based on quantum computers or on as-yet-undreamed-of computing methods.

In *MarpxPrivacy*, the user retains total control of the roster. Each entry in the list of confidants includes a confidant code. This code is known only to the particular pair or small team of confidants. The list (the roster) is carefully guarded so that others may not know its content. Control by confidants ensures that there is **no provision for lawful access** (no *back door* in the security industry's parlance).

In contrast, *Extreme Encryption* users register themselves at a web site and select their confidants there. That site is controlled by the enterprise that employs them. The enterprise oversees the distribution of rosters and PET (Private Exchange Tool) files. Access to rosters and PET files is the crucial factor in **provision for lawful access**, that can be initiated under controlled guidelines by enterprise leaders and their designees *and* in exceptional circumstances by a U.S. court.