On the morning of December 6, 2019, Mohammed Saeed Alshamrani opened fire in one of the classroom buildings at the Naval Air Station in Pensacola, Florida, killing three U.S. navy sailors and injuring eight more. On January 13th, 2020, Attorney General William Barr requested that Apple, in the interest of the investigation, provide technical assistance in circumventing the brute-force protections on Alshamrani’s iPhones. Apple would create a new iPhone operating system, which would prevent delays between password attempts and remove the auto-erase function, which entirely wipes the device after ten unsuccessful password attempts. This would allow the FBI to attempt all 10,000 possible combinations for the 4-digit pin until it gained access to the device. Apple, as in previous cases, refused to comply, arguing that doing so would give the Federal Bureau of Investigations the ability to compromise all iPhones, threatening the security and privacy of Apple users around the world.

The Pensacola case questions the trade-off between national security and freedom in the digital age. It does so in ways that are novel, intricate and perhaps more disturbing than ever before. This essay argues that strong encryption should not be weakened, because it enshrines political and moral freedom, and protects the rule of law. It explores technical options to satisfy law enforcement’s demands in unlocking devices while precluding sliding towards abusive surveillance. Finally, it offers lines of thought towards a global governance of encryption.

Defining Strong Encryption

Encryption is the process of converting data to an unrecognizable or “encrypted” form, in such a way that only authorized parties (parties that possess a key) may access it. Strong encryption refers to encryption methods that use long cryptographic keys (256 bits minimum), which are much longer to decrypt (Apple uses 256-bit AES). “At-rest” encryption refers to a technique which builds a unique identifier (UID) into a device and automatically encrypts all data (messages, photos, contacts, etc.) stored on that device. Strong encryption may also be applied to transiting data: “end-to-end” encrypted messaging apps such as WhatsApp, Telegram or Signal make it impossible for anyone but the communicating users to read conversations. In the below essay “weakening
encryption” refers to any action which may increase the ability of a third party to access plaintext, either through decryption, the acquiring of a key, or the circumvention of encryption protections.

**In Defense of Strong Encryption**

Strong encryption upholds three dimensions which are core to liberal democratic conception of freedom: free speech, privacy and transparency of law enforcement.

**Free speech**

Strong encryption is often the last bulwark of free speech, and as such it should be defended. Messaging apps have become a quasi-universal mode of communication. Politically oppressed minorities, as well as persecuted journalists, use encrypted messaging apps to bypass government surveillance. Weakening encryption would curtail their ability to express their beliefs, spread the word, convene, and take part in political life. The global trend towards authoritarian backsliding (Freedom House) should inspire defiance towards any weakening of encryption, but there is ground for defiance in liberal democracies, too. Breaches – real or supposed – into presidential candidates’ emails in the US (Hillary Clinton, 2016) and France (Emmanuel Macron, 2017) have been extremely disruptive to the democratic process. They could have exposed private communications to the public with devastating consequences. The first demand on any access to encrypted data should be that access be necessary and unambiguously beneficial to the public.

**Privacy**

The weakening of encryption does not threaten the freedom of political opponents only; it threatens everyone’s privacy and therefore everyone’s freedom. Indeed, the cryptographic key for a messaging app decrypt all communications transiting through that app. Similarly, the type of technical assistance the FBI requires from Apple would enable it to unlock all devices in its custody. The Snowden affairs have induced suspicion in many internet users (Stoycheff, 2016). Yet the mere perception that their communications may be monitored has a chilling effect on peoples’ expression of political or otherwise controversial views, experiments have shown (Penney 2016, Stoycheff, 2016). Exposure to surveillance may also incur more wide-ranging changes in behavior, causing people to become more fearful, more submissive. Being under constant scrutiny may indeed leave one’s sense of oneself as a person, one’s autonomy, vulnerable – and thus lessen one’s individual freedoms (Bloustein, 1964). A further requirement for government access would be that it must, by design, remain targeted.

**Transparency**

The secrecy of mass surveillance is perhaps its most distasteful feature. Our notion of privacy is intuitively grounded in a time when law enforcement was public, and your home could hardly be searched without your knowledge. Allowing for backdoors in messaging apps would approximate the Panopticon device imagined by Bentham in the eighteenth century: an institutional system which controls large groups of people by making it possible for them to be watched, without them knowing whether they are, in fact, being watched (Greenwald, 2016). The asymmetry between the publicity of the private individual’s actions on one hand, and the secrecy with which surveillance operates on the other hand, violates the rule of law and jeopardizes citizen’s freedom within the polity. A third requirement would be that surveillance, if necessary, be transparent.

Our intuitive understanding of freedom makes at least three demands on access to encrypted data by law enforcement: necessity, non-scalability, and transparency. Weakening encryption standards or circumventing encryption protections meet none of those demands.
Looking for a middle ground

Nevertheless, a case can be made for accessing locked devices in law enforcement’s custody, when information crucial to the investigation cannot be obtained by other means, and is key to national security (e.g., a terrorist attack). Allowing for data access without weakening encryption leaves few options: two proposals are reviewed below.

Distributed Key Escrow

Key escrow refers to a scheme where the keys needed to decrypt data are held in escrow so that an authorized third party may access the keys (National Academy of Sciences, 2018). One way to protect the key is to split it into pieces, each stored within a different organization. This approach reduces the risk of keys being stolen or appropriated by any third party. However, it has one may drawback: because it is not necessary to have physical custody of the device to unlock it, it may lead to surveillance abuses.

Hardware-Based Device-Level Key Escrow

Savage (2018) proposes to co-locate credentials in a hardware component that can only be interrogated after continued, 72-hour physical access. The hardware would provide access to the data only if the requestor produces evidence of judicial authorization through a device-specific secret. Each of these device-specific secrets would be maintained by the manufacturer. Notification of the intervention would be built into the procedure, so the owner of the device would know their data had been accessed. This proposal guarantees non-scalability, because unlocking requires a device-specific cryptographic key, which is “burnt” into the hardware during manufacturing and cannot be read by any software but that device’s security management system (similar to Apple’s Secure Enclave Processor). However, in this design, the manufacturer keeps the “authorization” keys, which raises several important questions. Are manufacturers able to securely maintain hundreds of millions of keys? Manufacturers already maintain single cryptographic keys for updates to their software – but the scale here would be much larger. More importantly, the design raises issues of trust. Do we trust manufacturers not to peek into our devices? Do we trust them never to yield to unwarranted demands from law enforcement?

In light of the challenges to the approaches above, there is no workable middle ground on allowing “exceptional” access to plaintext stored on an encrypted personal device. Other types of data, such as data stored on the Cloud or metadata remain accessible and largely unencrypted, however.

A corporate global governance of strong encryption

Relying on the private sector

It would be naïve to expect governments to bolster strong encryption, because of how close the topic is to their core equities, and because of a collective action problem (Deeks, 2016). Device manufacturers and messaging application providers are more likely to lead the way in defending encryption, because they own the technology, have the expertise, and are commercially motivated to do so. Indeed, users’ demands for privacy are on the rise, as evidenced by the success of Signal and Telegram, and switches to end-to-end encryption by WhatsApp (2016), Viber (2017), and Facebook Messenger (2016, optional). Moreover, yielding to government requests is costly: it takes time and resources, weakens reputation, and increases risk (e.g. in the event of a leak or data breach).

An International Trade Association of Encryption

Providers of encrypted services and devices may form a trade association dedicated to publishing and enforcing industry standards on strong encryption. International trade associations exist in numerous industries (e.g. Worldsteel for steel producers, IFPMA for pharmaceutical companies) and have a strong record in lobbying and norm diffusion. The
association would have two goals: (i) allowing companies to resist government demands by committing to strong encryption as an industry standard, (ii) avoiding collective action problems and their consequences on security. The core enforcement mechanism would rely on the integration of encrypted services with one another. Indeed, social media, email services and messaging apps are increasingly integrated with one another – for example, a professional LinkedIn account (Microsoft) can be integrated to Gmail (Google). Similarly, hardware manufacturers and software providers are interdependent, as the dispute between Google and Huawei demonstrated. Thus, any member who would refuse to abide by strong encryption rules would risk losing its integrations to key partners, greatly damaging its value proposition.

An Oversight Board
The association’s decisions would be informed, reviewed and validated by a board of trustees selected from a pool of users and experts. This institution would insure checks and balances on corporate members’ decisions. Such self-regulation is not unheard of in the technology space. By Summer 2020, Facebook will launch its Independent Oversight Board, the mission of which will be to improve the efficacy and relevance of content moderation policies. Similarly, the Oversight Board of the Association would be financially independent, with a multi-year endowment. Any of the Association’s proposals for standards would be submitted to the Board, which would be able to veto them with a qualified majority. The Board’s decisions would also inform the Association’s policies, as it attempts to keep up with new technologies that impact encryption. Forty part-time trustees would be selected from a pool of users, lawyers, engineers, and advocates of civil liberties from around the world.

Outstanding Challenges
Even if an international industry consensus is built on strong encryption, sovereign governments will retain their intelligence capabilities. The United States typically resorts to “lawful hacking”, i.e. using an exploit (typically a software or set of commands) to take advantage of existing vulnerabilities in devices or services. In the investigation of the San Bernardino attacks in 2015, the FBI purchased an exploit from an unnamed private provider, which circumvented the brute-force protections on the shooter’s iPhone (Kamps). Because the exploit remains secret, it is not known whether it could have been used to access other devices. The United States, through its Vulnerability Equities Policy, may choose not to disclose a vulnerability to a technology provider, if exploiting it is useful for intelligence purposes. This may mean that millions of users are exposed to a vulnerability that has not yet been patched. Moreover, relying on private providers such as Cellebrite or the NSO group, who sell their services at a hefty price (> $1.3 million for the San Bernardino exploit) may encourage a market for vulnerabilities which, if leaked, could jeopardize all devices’ security.

Conclusion
At its core, the encryption debate questions our relationship to freedom. How much freedom are we willing to trade against other goods, such as security or convenience? How much do we trust authority bearers (the State, the technology companies, the legal jurisprudence) to guarantee those trade-offs? It is unlikely that technological design, no matter how sophisticated, will ever answer these questions for us. I have argued that the mere technical possibility of surveillance extols intolerable costs on the individual’s ability to take part in public life, to think critically, and on their standing as a citizen – all crucial expressions of freedom that must be defended. Therefore, there is no credible alternative to strong encryption for the purpose of upholding individual freedoms in the digital age. One way to defend it would be for manufacturers of encrypted devices and providers of encrypted services to coalesce into an international trade association and build strong encryption into an industry standard.
References


