Why I attempted to find the middle ground in the on-going debate on governmental access to encrypted devices

The government wants the ability to quickly and easily access the personal and sensitive data stored on our encrypted devices

Background

On 2nd December 2015 the deadliest terrorist attack to take place on U.S. soil, since the 11th September 2001 attacks, occurred at the Inland Regional Center in San Bernardino, California. Fourteen people were killed, and twenty-two people were seriously injured, in a mass shooting by Syed Rizwan Farook and Tashfeen Malik, a married couple. The couple had targeted a training event and Christmas party of the San Bernardino County Department of Public Health, of which Farook was an employee. The number of dead and injured would likely have been much higher had the bombs that the couple had carried not been defective. A few hours later, after having the fled the scene of the shooting in a rented vehicle, the couple was killed in a shootout with police.

More information on the 2015 San Bernardino attack can be found here:
https://en.wikipedia.org/wiki/2015_San_Bernardino_attack

After the attack the Federal Bureau of Investigation (FBI) recovered an Apple iPhone 5C smart-phone belonging to San Bernardino County Department of Public Health, and which the department had previously issued to Farook. The FBI believed that this smart-phone contained valuable information related to the terrorist attack.

On 9th February 2016, the FBI announced that it was unable to unlock the smart-phone due to its advanced security features. The FBI then asked the National Security Agency (NSA) to unlock the phone, but they were also unable to do so. The FBI then requested Apple Inc., the manufacturer of the smart-phone, to create a new version of the smart-phone's operating system, iOS, which would disable certain of the smart-phone's security features, and, thereby allow the FBI to, eventually, unlock it. Apple declined this request, because it did not want to build a security backdoor into any of its products. A backdoor that they knew would never be used just once, as the FBI suggested it would be.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

On 16th February 2016, the FBI obtained a court order, issued under the All Writs Act of 1789, compelling Apple to comply. Apple responded, stating that they would oppose the order. Apple then published an open letter to its customers explaining why it had taken this particular course of action.

Apple's letter can be found here:
https://www.apple.com/customer-letter/

On 21st March 2016, the Department of Justice requested a delay in the court action it had initiated against Apple, because a third party had demonstrated a possible method for unlocking Farook's smart-phone. The delay was granted.

On 28th March 2016, the FBI announced that it had unlocked Farook's smart-phone with the aid of a third party.

On 7th April 2016, James Comey, Director of the FBI, explained that the tool that had been used to unlock Farook's smart-phone was only applicable to the Apple iPhone 5C and older Apple smart-phones that did not possess a Touch ID sensor. It is believed that the FBI purchased this tool from the third party for an estimated US$1.3 million.

Further information on the Apple-FBI Encryption Dispute can be found here:
https://en.wikipedia.org/wiki/FBI–Apple_encryption_dispute

On 11th March 2016, in the middle of the FBI's attempt to force Apple to 'help' unlock Farook's smart-phone, President Barack Obama was interviewed at South by Southwest (SXSW) Interactive by Evan Smith, the editor-in-chief of the Texas Tribune. The interview was wide ranging, and included a number of remarks relating to the subject of governmental access to encrypted devices. A selection of those remarks is now presented below:

> *"All of us value our privacy, and this is a society that is built on a Constitution and a Bill of Rights and a healthy skepticism about overreaching government power. Before smartphones were invented, and to this day, if there is probable cause to think that you have abducted a child, or that you are engaging in a terrorist plot, or you are guilty of some serious crime, law enforcement can appear before your -- at your doorstep and say, we have a warrant to search your home, and they can go into your bedroom and into your bedroom doors and rifle through your underwear to see if there's any evidence of wrongdoing."*
>
> *"And we agree on that, because we recognize that just like all of our other rights -- freedom of speech, freedom of religion, et cetera -- that there are going to be some constraints that we impose in order to make sure that we are safe, secure and living in a civilized society."*
>
> *"Now, technology is evolving so rapidly that new questions are being asked. And I am of the view that there are very real reasons why we want to make sure that government cannot just willy-nilly get into everybody's iPhones that is full of -- or smartphones that are full of very personal information and very personal data. And let's face it, the whole Snowden disclosure episode elevated people's suspicions of this. So does popular culture, by the way, which makes it appear as if I'm in the Sit Room and I'm moving things."*
>
> *"But I understand that that raised suspicions. All right. So we're concerned about privacy. We don't want government to be looking through everybody's phones, willy-nilly, without*

any kind of oversight or probable cause or a clear sense that it's targeted at somebody who might be a wrong-doer."

"What makes it even more complicated is the fact we also want really strong encryption, because part of us preventing terrorism, or preventing people from disrupting the financial system or our air traffic control system or a whole other set of systems that are increasingly digitalized is that hackers, state or non-state, can just get in there and mess them up. So we've got two values, both of which are important. Right?"

"And the question we now have to ask is, if technologically, it is possible to make an impenetrable device or system where the encryption is so strong that there's no key, there's no door at all, then how do we apprehend the child pornographer? How do we solve or disrupt a terrorist plot? What mechanisms do we have available to even do simple things like tax enforcement? Because, if, in fact, you can't crack that at all, government can't get in, then everybody is walking around with a Swiss bank account in their pocket -- right? So there has to be some concession to the need to be able to get into that information somehow."

"Now, what folks who are on the encryption side will argue is any key whatsoever, even if it starts off as just being directed at one device could end up being used on every device. That's just the nature of these systems. That is a technical question. I'm not a software engineer. It is, I think, technically true, but I think it can be overstated."

"And so the question now becomes, we as a society -- setting aside the specific case between the FBI and Apple, setting aside the commercial interests, concerns about what could the Chinese government do with this even if we trusted the U.S. government -- setting aside all those questions, we're going to have to make some decisions about how do we balance these respective risks."

"And I've got a bunch of smart people sitting there, talking about it, thinking about it. We have engaged the tech community aggressively to help solve this problem. My conclusion so far is that you cannot take an absolutist view on this. So if your argument is strong encryption, no matter what, and we can and should, in fact, create black boxes, then that I think does not strike the kind of balance that we have lived with for 200, 300 years. And it's fetishizing our phones above every other value. And that can't be the right answer."

"I suspect that the answer is going to come down to how do we create a system where the encryption is as strong as possible, the key is as secure as possible, it is accessible by the smallest number of people possible for a subset of issues that we agree are important. How we design that is not something that I have the expertise to do."

"But I caution -- I am way on the civil liberties side of this thing. Bill McRaven will tell you that I anguish a lot over the decisions we make in terms of how to keep this country safe, and I am not interested in overthrowing the values that have made us an exceptional and great nation simply for expediency. But the dangers are real. Maintaining law and order and a civilized society is important. Protecting our kids is important. And so I would just caution against taking an absolutist perspective on this."

"Because we make compromises all the time. I haven't flown commercial in a while but my understanding is it's not great fun going through security. But we make the concession because -- it's a big intrusion on our privacy, but we recognize it as important. We have

> *stops for drunk drivers. It's an intrusion, but we think it's the right thing to do. And this notion that somehow our data is different and can be walled off from those other tradeoffs we make I believe is incorrect."*
>
> *"We do have to make sure, given the power of the Internet and how much our lives are digitalized, that it is narrow and it is constrained and that there's oversight. And I'm confident this is something that we can solve. But we're going to need the tech community -- software designers, people who care deeply about this stuff -- to help us solve it."*
>
> *"Because what will happen is if everybody goes to their respective corners and the tech community says, you know what, either we have strong, perfect encryption, or else it's Big Brother and an Orwellian world -- what you'll find is that after something really bad happens, the politics of this will swing and it will become sloppy and rushed, and it will go through Congress in ways that have not been thought through. And then you really will have dangers to our civil liberties because we will have not done -- the people who understand this best and who care most about privacy and civil liberties have sort of disengaged or taken a position that is not sustainable for the general public as a whole over time."*

A complete transcript of President Barack Obama's remarks from his SXSW Interactive interview can be found here:
https://obamawhitehouse.archives.gov/the-press-office/2016/03/14/remarks-president-south-southwest-interactive

Middle ground

I agree with much of what President Obama said during that interview. I believe that a genuine and justifiable need for governmental access to encrypted devices does exist, and that if the global information technology community does not voluntarily devise a mechanism for this to happen then the governments of the world will force one on us instead, which, I can assure you, is a situation that really should be avoided at all costs. Why? Because any government-devised mechanism will probably be driven more by the extreme views of political hawks than by the moderate views of political doves, which is likely to give the government far more than it actually needs, instead of the absolute bare minimum required to adequately respond to the most exceptional of circumstances. So, if we want a mechanism for governmental access to encrypted devices that is largely-acceptable, instead of one that is largely-unacceptable, then we need to wake up, smell the coffee, and quickly start to do something about it, because this problem is not going to go away any time soon.

Some, perhaps many, would say that believing that there is a genuine and justifiable need for governmental access to encrypted devices is naive, foolish and, possibly, even downright dangerous. I completely understand such views, and it is because I completely understand such views that I know, beyond a shadow of a doubt, that the only possible solution to this problem is going to be one that cannot be abused in any way, shape or form by criminals, dictators, hackers, lunatics, overzealous 'democratic' governments, rogue nation states, terrorists, totalitarian regimes or even its own operators.

I believe that a practical solution is both possible and worthwhile. But, I do not believe that such a solution will be simple, easy or cheap. In all likelihood, it will be technically complex, highly challenging and very expensive. A collection of characteristics, which, at first glance, would seem

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

to be highly unfavorable, but which, with just the right sort of solution, might actually be turned to our significant advantage.

For those that oppose such beliefs, the dangers are clear, and what I suggest should not even be contemplated, let alone spoken of out loud. For such people, it is their innermost thoughts that are at risk of being publicly exposed, and as they will eloquently explain, everyone has secrets that they would prefer to keep perpetually hidden. They will also point out that the road to hell is paved with many good intentions, and that this particular good intention should definitely be left well enough alone. I can totally understand this viewpoint, but I can also totally understand that the government, in the most exceptional of circumstances, would greatly benefit from being able to decrypt a suspected criminal or terrorist's encrypted device.

Now, whilst I may appear to be fully on the side of the government in this matter, I can assure that I am not. I honestly feel that I sit squarely in the middle, in that gray area that exists between black and white. I do not want everyone's privacy undermined. I do not want to give the governments of the world free reign to be able to easily access everyone's personal or sensitive data without so much as a by-your-leave. I do not trust the governments of the world to sanely or safely operate any solution that may be devised for governmental access to encrypted devices. I believe that any solution will require fully-independent non-governmental global oversight. I also believe that the use of any solution must always be restricted to the most exceptional of circumstances. I do not want any solution to be easy, quick or cheap to use. I want it to be hard, slow and expensive. I want its use to be hotly debated and fully-considered before each and every time that it is used. I want its use to be open, in the light, and not hidden, in the shadows. I want it to be a tool for good, not a tool for evil. I want it to be done right, or not at all, which is perhaps the most important view I can possibly express on this subject. Providing governmental access to encrypted devices is not some sort of theoretical consideration of little consequence. This is the most serious of subjects, and any solution that does get created will have highly-significant long-lasting implications. It might release an omnipotent genie from its bottle, one that may be impossible to ever recapture. Therefore, it must be done correctly, because the implications of getting it wrong are unthinkable.

So, you can see that I know what I want and what I don't want. Of course, what I want, or don't want, may be completely unobtainable, but I do not see why that should be the case. This is undoubtedly a highly-complex problem but not one that is so complex or intractable that it is genuinely beyond the wit of humanity to solve. Particularly in world that already contains so many highly-secure mission-critical systems.

Previous attempts at solving the governmental access to encrypted devices problem have involved ideas such as putting a government-controlled backdoor into our encryption algorithms, or allowing the government to hold a copy, in escrow, of all our encryption keys. The first utterly undermines the security and privacy of everyone that uses such algorithms, and the second creates an irresistible honey-pot for criminals, dictators, hackers, lunatics, overzealous 'democratic' governments, rogue nation states, terrorists and totalitarian regimes.

There has to be a better way, and because I believe that a better way actually exists that I decided to propose a solution (see Stake in the Ground, below). I must stress that my proposed solution is not implementation-ready; it is only discussion-ready, and no more. It is intended to start a calm and measured conversation within the global information technology community about how to solve the governmental access to encrypted devices problem in a balanced and reasonable way. It tries to find a middle ground; a pragmatic solution that will be acceptable to the majority of interested parties. Obviously, any middle-ground type of solution is never going to appeal to those that hold the most extreme views on this subject. Those that want complete and unfettered access to encrypted devices

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

will be disappointed that access, whilst possible, is severely limited. Those that do not want any access at all will be disappointed that even severely-limited access is possible. It is just not going to be possible to please everyone, and certainly not the minority that hold unwavering views at the extremes. The only sensible approach is going to be some sort of a compromise that is more or less acceptable to the moderate majority. The trick in appealing to this majority will be to devise a solution that can only be used in the most exceptional of circumstances and is under fully-independent non-governmental control. All I can do is try to start that conversation and hope that the voices of the moderate majority do not get drowned out by the voices of the extreme minority. I do not think that it is wrong to hope such things. It is also important to understand that my proposed solution, as it currently stands, undoubtedly raises far more questions than it answers, and it will only be through such conversation that all pertinent questions will be raised, adequately considered and appropriately answered.

Foreground

As President Obama remarked at SXSW:

> *"Because what will happen is if everybody goes to their respective corners and the tech community says, you know what, either we have strong, perfect encryption, or else it's Big Brother and an Orwellian world -- what you'll find is that after something really bad happens, the politics of this will swing and it will become sloppy and rushed, and it will go through Congress in ways that have not been thought through. And then you really will have dangers to our civil liberties because we will have not done -- the people who understand this best and who care most about privacy and civil liberties have sort of disengaged or taken a position that is not sustainable for the general public as a whole over time."*

So, it seems clear that we now need *"the people who understand this best and who care most about privacy and civil liberties"* to creatively and pragmatically reengage with this problem, and start to devise a largely-acceptable solution before *"the politics of this will swing and it will become sloppy and rushed, and it will go through Congress in ways that have not been thought through"* and we end up with a largely-unacceptable solution.

Of course, I would greatly prefer that we lived in a world where no solution was necessary at all, but sadly we don't; as has been clearly demonstrated by the San Bernardino attack in 2015 and the 9/11 attacks in 2001. So, given a choice between a voluntarily-adopted solution based on a hopefully-narrow and inflexible design, from a danger-aware and, therefore, highly-cautious global technology community, for use in only the most exceptional of circumstances, and a legally-imposed solution based on a potentially-broad and open-ended design, from an overly-confident and technologically-illiterate hawkish-government, for use whenever it is politically beneficial, I have to choose the least-worse solution, which is obviously the narrow and inflexible one designed by a highly-cautious global technology community for voluntary adoption that can only be used in the most exceptional of circumstances.

I think you will agree that it is better to have some say in this matter than no say at all, and it is for this reason, more than anything else, that I attempted to find the middle ground in the on-going debate on governmental access to encrypted devices.

Stake in the ground

Governmental access to the personal and sensitive data stored on our devices needs to be very carefully controlled

My proposal describes, at a high level, and in the broadest of terms, a pragmatic approach to facilitate 'limited-governmental access to encrypted devices'. A key objective of this proposal was to make such access possible but not cheap or easy. This proposal is not an implementation-ready design, and only addresses the extraction of data-at-rest from an encrypted device, and not the extraction of data-in-motion from an encrypted communications channel. It is hoped that this proposal will catalyze global discussions on the subject and eventually lead to a practical solution that is acceptable to all interested parties.

Please bear the following in mind when reading the proposal. The two most important statements in the previous paragraph were: *'this proposal is not an implementation-ready design'*, and *'it is hoped that this proposal will catalyze global discussions on the subject'*. So, as far as I am concerned, at this point in time, it is far more important to get the global technology community talking about the problem of governmental access to encrypted devices than it is to agree on any particular solution.

- Limited-Governmental Access To Encrypted Devices (proposal) V2.0.pdf:
- *http://docdro.id/XnCcNMa*
- MD5: c4a9be9b41aa5b30de65922550cbd99d

This proposal is based on a large number of assumptions, some of which are listed in the appendix (below), along with explanations of why I believe those assumptions are reasonable.

Appendix

In general, the reason that I believe that the following assumptions are reasonable is because if you breakdown the problem of governmental access to encrypted devices into its more primitive elements then it can be clearly seen that many of the tools, techniques and technologies that will be required to build those elements are already mature and field-proven across a wide range of industries. Industries that often depend on highly-secure mission-critical systems, built from those exact same tools, techniques and technologies, in order to operate in even in a minimally-acceptable manner. Therefore, it seems reasonable to assume that if it was possible to build such systems from such tools, techniques and technologies in the past then it will be possible to do so again in the future, as we attempt to find a largely-acceptable solution to the governmental access to encrypted devices problem.

It should be noted that the following assumptions are not perfectly reasonable, only sufficiently reasonable, and it is on that basis that I proceeded to create a proposed solution to this problem. Obviously, it would have been far better if all my assumptions had been perfectly reasonable but that may not be possible given the nature of this particular problem, and sufficiently-reasonable assumptions may be the best that will ever exist. Proceeding on this basis has allowed a new solution to be proposed, which may encourage others to look at this problem in fresh new ways that will, in turn, eventually lead to the creation of the largely-acceptable solution that we ultimately seek.

Assumption #1: Providing limited-governmental access to encrypted devices (L-GATED) is both necessary and reasonable in the most exceptional of circumstances.

Why this assumption is reasonable: There are definitely exceptional circumstances in which a national government would clearly benefit from being able to access the data stored on an encrypted device belonging to a criminal or terrorist. Without such access a national government would clearly have less information available to either prevent a crime or terrorist act from taking place, or to investigate a crime or terrorist act after it had occurred. Therefore, commonsense dictates that providing limited-governmental access to encrypted devices in the most exceptional of circumstances is both necessary and reasonable. Of course, providing such access has a number of very serious implications, which any L-GATED solution must acceptably address.

Assumption #2: That a technically-simple solution to the limited-governmental access to encrypted devices (L-GATED) problem is not possible, otherwise such a solution would already have emerged from the global information technology community and, therefore, a technically-complex solution is very likely the only solution that is possible.

Why this assumption is reasonable: After many years of looking for a technically-simple solution to the L-GATED problem none has (apparently) ever been found. We should, therefore, now consider the very real possibility that such a solution does not, in fact, exist, and that the only solution that is ever going to be possible is a complex one. Many modern systems are technically complex, including the on-board flight systems that help to keep aircraft safely in the sky and the air-traffic control systems that manage the simultaneous take-off and landing of multiple aircraft at busy international airports. The challenge of such mission-critical systems could only be solved by a technically-complex solution, and the solution to the L-GATED problem is likely to be no different.

Assumption #3: That the risks associated with a limited-governmental access to encrypted devices (L-GATED) solution can be reduced to an acceptable level.

Why this assumption is reasonable: The solution to the L-GATED problem is very likely to be a complex one. There is nothing inherently wrong with complex solutions per se. Of course, such solutions are, by their very nature, more challenging to develop and maintain, which means that such solutions often have higher risks associated with them than simpler solutions. However, just because a potential solution has increased risks does not mean that it should not be considered a viable solution. Often a concerted effort to understand and manage such risks can lead to a significant reduction in the likelihood that those risks will ever occur and a significant reduction in the impact of those risks if they do occur. Many existing systems, such as the on-board flight systems that help to keep aircraft safely in the sky and the air-traffic control systems that manage the simultaneous take-off and landing of multiple aircraft at busy international airports are technically complex. Such systems are in active use only because sufficient time and effort has been spent reducing the risks associated with those systems to acceptable levels. So, with sufficient time and effort the risks associated with an L-GATED solution can, like the risks associated with other technically-complex high-risk systems, be reduced to an acceptable level, ensuring that a catastrophic failure is almost impossible.

Assumption #4: National governments cannot be trusted to manage the use of a limited-governmental access to encrypted devices (L-GATED) solution.

Why this assumption is reasonable: National governments are responsible for gathering data related to criminal and terrorist activity, if they also had responsibility for managing the use of an L-GATED solution within their own borders then it could easily lead to a situation where the overzealous pursuit of the former could lead to abuses of the latter. To put it simply, being able to easily access the data stored on any citizen’s device, something that they cannot currently do, would be too much of a temptation for most, if not all, national governments, the use of which would quickly become a commonplace everyday occurrence, rather than something reserved for only the most exceptional of circumstances. Additionally, what a country's government can, or cannot, do should be controlled by laws. The publishing of those laws allows the citizens of that country to understand what their government can, or cannot, do. However, many national governments enact secret laws, which are, obviously, not published, and are therefore beyond public understanding. Some laws even prohibit public notification of their use. This allows a national government to potentially do many things that its citizens would probably not approve of, such as legally abusing the use of an L-GATED solution, as just described. It is for such reasons, and probably many more, that national governments cannot be trusted to manage the use of an L-GATED solution.

Assumption #5: That a non-governmental organization should manage the use of the limited-governmental access to encrypted devices (L-GATED) solution.

Why this assumption is reasonable: If the national governments of the world cannot be trusted to manage (oversee) the use of an L-GATED solution (see point 4), then it would seem that the only viable alternative is for a non-governmental organization to take that responsibility. By appointing a non-governmental organization to oversee the use of the L-GATED solution the potential for governmental abuse of that solution (see point 4) will be greatly reduced, or even completely removed. Such an organization can be all the things that a typical national government cannot; independent, multi-national, open, and unbiased. This organization would then be able to ensure that the L-GATED solution was only used, in a highly controlled manner, in the most exceptional of circumstances. It is for such reasons that non-governmental oversight of the L-GATED solution is inherently better than governmental oversight, and that a non-governmental organization should manage the use of the L-GATED solution.

Assumption #6: That an independent non-governmental organization charged with overseeing the use of the limited-governmental access to encrypted devices (L-GATED) solution can be truly independent.

Why this assumption is reasonable: It should be possible to create an organization that is able to function independently of any national government. This could be achieved through the use of four key approaches; virtualization, openness, audit and the creative use of tools, techniques and technology. Virtualization: The organization will be virtualized. It will be globally distributed and will only exist in a logical sense, and not a physical one. Consequently, it will transcend all national borders, and the laws associated with such borders. It will be staffed by people united by purpose and belief from all around the world, and its computational resources will be supplied by the cloud. The staff and its systems will communicate via encrypted communications carried over the dark web. The organization will exist everywhere and nowhere, and should, consequently, be wholly independent of any national government. Openness: The operation of the organization will be open. Its software systems will make extensive use of open-source software that can be inspected to determine acceptable design. The design of any custom systems developed by the organization will be published on an open-source basis. The organization will publish, in real time, high-level information about its operation, which will then allow the general public to determine whether or not the capabilities of the organization are being used as intended. It should be noted that this openness is unlikely to extend to the personal details of its staff or the physical location of its systems, both of which will need to be kept private in order to ensure that its staff are protected from governmental persecution and to ensure the security of the device-related data stored within its systems. So, given that the organization will be designed to operate independently of any national government, such openness will help to ensure that the organization does, in fact, operate wholly independently of any national government. Audit: The organization will submit to regular audits of its technical and manual systems by an independent third party. The independent third party will be a respected entity in the field of systems audit. The third party will publish its findings for all to see. So, given that the organization will be designed to operate independently of any national government, such audits will help to ensure that the organization has been designed to and does, in fact, operate wholly independently of any national government. Tools, techniques and technology: As the operation of the organization will undoubtedly depend on people that are beholden to the laws of their respective national governments, the organization's independence from such national governments cannot be totally assured. This is where the creative use of tool, techniques and technology comes into play. The organization will assume that its staff cannot be trusted, and may be under governmental control. This will not be a malicious mistrust but a realistic one, because it is simply not possible to know with absolute certainty that any individual that works for the organization can be trusted absolutely. A better approach is to assume that all of the organization's staff cannot be trusted at all and to create a framework of tools, techniques and technologies within which the organizations' staff is only able to contribute towards the correct operation of the organization and is, consequently, actively prevented from doing otherwise. This does not mean that no member of the organization will be trustworthy, only that the required operation of the organization will not be critically dependent on such a character trait. By ensuring that an organization's tools, techniques and technologies can only be used in the ways that they were intended to be used by the organization it should be possible to ensure the correct and independent operation of the organization, regardless of whether or not its staff are under governmental control. So whilst the organization's staff may not be foolproof, its systems will be. Of course, the trick will be to design a system that cannot be easily sabotaged or subverted. Some of the tools, techniques and technologies that could be used to help build such a system include: activity logging, biometric scanners, compartmentalization of information, critical function automation, dark web, defense in depth, double-blind consensus-based decision-making, encryption, failsafe design, fundamental distrust of the human element, hidden services, identity and access management, multi-factor authentication, not-for-profit business model, operational analysis, perpetual war footing, physical decentralization, principle of least privilege, redundantly-staffed roles, risk management, security through obscurity, segregation of duties, subject matter experts and a systems design based on a finite state machine, to name but a few. Of course, at the end of the day it will never be possible to absolutely ensure that an organization will be able to operate wholly independently of any national government, but the approaches of virtualization, openness, audit and the creative use of tools, techniques and technology described above should allow the creation of an organization that is, at a minimum, acceptably so.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

Assumption #7: It will be possible to restrict use of the limited-governmental access to encrypted devices (L-GATED) solution to only approved governmental entities.

Why this assumption is reasonable: It should be possible to devise an L-GATED solution that will be able to restrict its use to only approved governmental entities and to no one else. This could be achieved through the requirement that all L-GATED solution users must meet stringent criteria before they are allowed to use the solution. Anonymous use of the L-GATED solution will not be allowed. This is because the L-GATED solution is intended to be a tool for good, that will only be used in the light, for all to see, and not a tool for evil, the use of which can be hidden from view in the shadows. If a user meets all required criteria then they will become an approved L-GATED solution user. Multi-factor authentications (what you know, have and are) will be set up for each approved user. Every use of the L-GATED solution will require multi-factor authentication. All user interactions with the L-GATED solution will take place over a secure communications channel. Use of this secure communications channel will be the only way that the L-GATED solution can be accessed. All user interactions over this channel will be logged. Use of the L-GATED solution will not be fully automated, as it will be necessary for a user to electronically interact with the staff of the fully-independent non-governmental organization that is expected to be responsible for overseeing the use of the L-GATED solution. Each use of the L-GATED solution will be carefully validated by the staff of this organization. It is also expected that only approved L-GATED solution users will be able to obtain the legal documentation from nation-level judicial authorities that will be necessary to use the L-GATED solution. So, by using such approaches it will be possible to restrict use of the L-GATED solution to only approved governmental entities.

Assumption #8: It is possible to devise a limited-governmental access to encrypted devices (L-GATED) solution that does not support mass surveillance.

Why this assumption is reasonable: It should be possible to design an L-GATED solution in such a way that it cannot be easily used for mass surveillance. As currently envisioned, the L-GATED solution will use at least five safeguards to prevent such a use. Firstly, use of the L-GATED solution will incur substantial capital costs, primarily because it will require the use of a highly-capable computational resource. The capital costs are expected to be so high that a national government will only be able to justify owning one such resource. Secondly, use of the L-GATED solution will incur substantial operational costs, primarily in terms of the energy required to operate the highly-capable computational resource. Thirdly, use of the L-GATED solution will be time consuming due to the fact that unavoidable time delays will have been purposefully built into its operation. One of these time delays will be due to a computational challenge that will require the use of a highly-capable computational resource in order to solve it in a reasonable timeframe. Fourthly, use of the L-GATED solution will be overseen by a fully-independent non-governmental organization. Any attempt to use the solution in an excessive manner, such as for mass surveillance, will be immediately detected and prevented by this organization. Fifthly, use of the L-GATED solution will require that the device to be decrypted is in the legal physical-possession of the national government that wishes to decrypt it. Together, these five safeguards should make using an L-GATED solution for mass surveillance wholly impractical.

Assumption #9: It is possible to devise a limited-governmental access to encrypted devices (L-GATED) solution that cannot be used surreptitiously.

Why this assumption is reasonable: It should be possible to devise an L-GATED solution that cannot be used surreptitiously (in secret). As currently envisioned, the L-GATED solution will use at least five safeguards to prevent such a use. Firstly, use of the L-GATED solution will require that the encrypted device is in the legal physical-possession of the national government that wishes to decrypt it. If the owner of an encrypted device keeps that device physically secure then it will be almost impossible to secretly decrypt it. An apparently missing, confiscated or stolen device must always be assumed to have been secretly decrypted until it is recovered and proven to be otherwise. Secondly, the L-GATED solution will purposefully not support the remote decryption of an encrypted device, as far as it is practical to do so. This will make the secret application of the L-GATED solution impossible, as it will not be possible to secretly apply the solution from a hidden location via a communications channel. One of the ways that this will be achieved is that applying the L-GATED solution to an encrypted device will require the use of an electronic interface that can only be accessed by physically disassembling that device. Thirdly, use of the L-GATED solution to decrypt an encrypted device will require legal authorization issued by nation-level judicial authorities. Whilst many judicial authorities are often happy to work in secret to prevent or investigate a serious crime or terrorist act they generally prefer to operate in a more open manner, so that justice can be clearly seen to be done. Consequently, they are unlikely to approve the secret use of the L-GATED solution. Of course, this cannot be taken for granted. Fourthly, use of the L-GATED solution will be subject to the approval and cooperation of a fully-independent non-governmental organization that will be charged with ensuring that use of the solution not is hidden from view, in the shadows, but is only used openly, in the light. Fifthly, any attempt to apply the L-GATED solution to an encrypted device will be securely logged on that device, and that log will be reported to the device's owner each time that device is restarted. So, any secret application of the L-GATED solution will (eventually) be discovered by the device's owner. Whilst none of these safeguards alone can perfectly assure that the L-GATED solution cannot be used surreptitiously; together they should be able to offer acceptably-imperfect assurance that this will not be the case in practice.

Assumption #10: It is possible to devise a limited-governmental access to encrypted devices (L-GATED) solution that does not weaken or invalidate any encryption algorithm.

Why this assumption is reasonable: The L-GATED solution will not be based on a weakened-lock approach (encryption algorithms with governmental backdoors); it will be based on the creative use of (encryption) keys. By devising an L-GATED solution that is based on the creative use of encryption keys it will not be necessary to alter, and thereby weaken or invalidate, any new or existing encryption algorithm. This is a hugely important ability because there will many instances where new or existing encryption algorithms will need to be used outside of the L-GATED solution.

Assumption #11: It is possible to devise a limited-governmental access to encrypted devices (L-GATED) solution that is compatible with a wide range of current and future encryption algorithms.

Why this assumption is reasonable: By devising an L-GATED solution that is based on the creative use of encryption keys, a feature that is common to all encryption algorithms, it will be possible to ensure that the solution is compatible with a wide range of current and future encryption algorithms. This is important because it is expected that, in the future, quantum computers will be able to easily decrypt, by force, data that has been encrypted with many currently-used encryption algorithms, and when that happens it will be necessary for the world to change over to encryption algorithms that are immune to quantum computer-based decryption attacks. Therefore, an L-GATED solution that can work with a wide range of new and existing encryption algorithms will be able to quickly respond to new decryption threats as and when they arise.

Assumption #12: It is possible to devise a limited-governmental access to encrypted devices (L-GATED) solution that can be selectively targeted at one class of devices, such as those used

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

by non-governmental users, and selectively excluded from another class of devices, such as those used by governmental users.

Why this assumption is reasonable: An L-GATED solution that is based on the inclusion of specific hardware and software within a particular class of devices will allow the L-GATED solution to be selectively applied, such that non-governmental users of one class of device can be easily included, whilst governmental users of another class of device can be easily excluded (or vice versa). This selectivity will allow the L-GATED solution to be applied to the devices used by ordinary citizens whilst being excluded from devices used by the judiciary, government officials, police, and military (or the other way around, if so desired).

Please note: Such selectivity would not only allow the L-GATED solution to be applied to specific classes of device it would also allow for the use of some creative business models. For example, a patriotic device manufacturer could include the L-GATED solution into all its non-governmental class devices as standard. It could then charge a premium for all governmental class devices that did not include the solution. This would then allow the manufacturer to recover, in part or in full, any extra costs that may have been incurred by including the solution into the non-governmental class devices directly from the entity that stands to gain the most from that inclusion, namely the national government. So, the national government would be able to access data stored on encrypted devices in only the most exceptional of circumstances, and the device manufacturer would not be unduly burdened by its decision to patriotically support the use of the L-GATED solution. Governmental users pay a bit more, non-governmental users pay the same, and the national government is better able to protect the nation.

Assumption #13: It is possible to devise a limited-governmental access to encrypted devices (L-GATED) solution that is only applicable to data-at-rest within an encrypted device and not to data-in-motion over an encrypted communications channel.

Why this assumption is reasonable: The currently envisioned L-GATED solution will be specifically designed to decrypt data-at-rest on an encrypted device that had been encrypted using a single static encryption key. This solution would, therefore, be unable to decrypt data-in-motion over a variety of encrypted communications channels, which would very likely use multiple dynamically-generated session-based encryption keys. This is important because the L-GATED solution is only intended to be a solution to the narrow governmental access to encrypted devices problem, and not the much broader governmental access to encrypted communications problem as well. The former is a largely-acceptable response to the most exceptional of circumstances, whilst the latter would be a largely-unacceptable tool of a totalitarian police state. The difference between such capabilities is well understood and will be purposefully factored into the design of the L-GATED solution, such that the solution will only be suitable for its single intended use, and no more.

Please note: An L-GATED solution could be used to gain access to data previously sent over an encrypted communications channel if an encrypted device was decrypted using that solution and the device contained a store of the data that had previously been sent over that channel. Additionally, dependent on the nature and state of the device's encrypted communications mechanism it may then be possible to actively communicate using that mechanism.

Assumption #14: That time delays can help restrict the use of the limited governmental access to encrypted devices (L-GATED) solution to only the most exceptional of circumstances.

Why this assumption is reasonable: The purposeful inclusion of unavoidable time delays into the L-GATED solution will be able to limit the rate at which it is used. Such delays can be implemented in a number of different ways, including manually by a human worker, programmatically by a hardware/software-based timer or through the use of a non-trivial computational challenge, which can only be solved in a reasonable period of time by a highly-capable computational resource. The main reason that the use of the L-GATED solution will be slowed in this way is to prevent its use for mass surveillance, which would probably require the decryption of a significant number of encrypted devices in a relatively short period of time. The time delays within the L-GATED solution are intended to severely limit how many encrypted devices can be decrypted within a given period of time. Thereby ensuring that its use will have to be highly selective, and it is hoped that this selection process will restrict its use to only the most exceptional of circumstances. As the capabilities of computational resources increase over time the L-GATED solution will need to proportionally increase its computational challenge, ensuring that acceptably-long time delays are always maintained. One particular computational challenge that would be suitable for use with an L-GATED solution would be a brute-force decryption attack on data that had been encrypted using a symmetric-key encryption algorithm. Determination of the encryption key required to decrypt such data would require the systematic testing of large numbers of speculatively created keys; a process that becomes more time consuming as the length of the encryption key increases. So, by selecting a sufficiently-long encryption key a sufficiently-long time delay can be obtained, even when using the most-capable computational resources currently available. Of course, such a time delay cannot be precisely defined, as it is dependent on the capabilities of the computational resource employed to solve the computational challenge. Consequently, such a time delay can only be broadly defined based on the use of the most-capable computational resource currently available. For example, using the world's fastest supercomputer an unavoidable time delay of approximately 24 hours can be expected. The use of a less-capable computational resource would, therefore, be expected to incur a larger time delay.

Please note: The use of unavoidable time delays by the L-GATED solution is just one of the ways that it will attempt to prevent its use for mass surveillance; the others are through capital costs, operational costs, oversight, and physical device access. Please see Assumption #8 for further details. It is believed that, to date, the largest key that has ever been found using a brute-force attack was a 64-bit version of the RC5 symmetric-key block cipher, which took just under 5 years, and was undertaken by distributed.net, a distributed-computing initiative governed by the non-profit organization Distributed Computing Technologies, Incorporated (DCTI). Of course, this attack took place in the public domain; hence our knowledge of it, but many other successful brute-force attacks have undoubtedly taken place behind the closed doors of the world's national security agencies. It is probably reasonable to assume that the computational resources that such agencies are able to dedicate to such attacks is likely to exceed those available to distributed.net by many orders of magnitude. Consequently, it is currently 'best practice' to assume that it is now practical to brute-force attack all encryption keys less than 90 bits. Distributed.net is currently attempting to brute force a 72-bit RC5 key, which, based on the progress made over the 14 years since the start of the attack in 2002, will take a total of (up to) 318 years to complete. In practice, this brute-force attack is likely to take much less time, due to improvements in the computational resources used for the attack that are expected to occur during the lifetime of the attack. In fact, because some improvements have already occurred, it is now expected that the attack will take no more than (up to) 179 years at its current rate of progress. Further improvements in the computational resources used for the attack are expected to reduce this figure even more in the future. It is believed that brute-forcing a 128-bit key will be impractical, not simply because of the unbelievable amount of time that it would take, but also because of the phenomenal amount of energy that would be required, even when using a computational resource that operates at the Landauer Limit. So, any keys larger than this, such as the 256-bit keys commonly used to achieve strong encryption via the

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

Advanced Encryption Standard (AES), will not just be impractical to brute force they will be utterly impossible. The L-GATED solution will use 256-bit encryption keys to encrypt a device. The L-GATED solution's unavoidable time delay will be obtained from a computational challenge that uses an encryption key that is approximately 80 bits in size. The size of this key will need to increase over time to counter improvements in the capabilities of computational resources that are expected to occur in the future. The duration of the solution's unavoidable time delay will be broadly tunable based on the number of bits in this encryption key.

More information on brute-force attacks can be found here:
https://en.wikipedia.org/wiki/Brute-force_attack

More information on the RC5 symmetric-key block cipher can be found here:
https://en.wikipedia.org/wiki/RC5

More information on distributed.net can be found here:
https://en.wikipedia.org/wiki/Distributed.net

More information on distributed.net's attempt to brute force a 72-bit key can be found here:
http://www.distributed.net/RC5/en

More information on the Landauer Limit can be found here:
https://en.wikipedia.org/wiki/Landauer%27s_principle

Assumption #15: That capital expense can help restrict the use of the limited governmental access to encrypted devices (L-GATED) solution to only the most exceptional of circumstances.

Why this assumption is reasonable: If the capital expense required to make use of the L-GATED solution is high enough then it will be able to help restrict the use of that solution to only the most exceptional of circumstances. This could be achieved through the use of a substantial computational challenge that would require the use of a highly-capable computational resource that is able to solve the challenge in a reasonable timeframe. If the computational challenge was made sufficiently hard then a highly significant capital expense would be required to purchase/build just a single instance of such a resource. Ideally, the computational challenge would be made so hard that no national government could sensibly justify owning more than one such resource. The capabilities of a single computational resource, even a highly capable one, are always going to be finite, which means that it will only be possible to use the L-GATED solution to decrypt a limited number of encrypted devices within a given period of time. Therefore, the use of that computational resource will have to be highly selective, and it is hoped that the selection process will be based on the existence of only the most exceptional of circumstances. So, the significant capital investment that will be required to make use of the L-GATED solution can help to restrict its use to only the most exceptional of circumstances**.** As the capabilities of computational resources increase over time the L-GATED solution will need to proportionally increase its computational challenge, ensuring that a significant capital investment will always be required.

Please note: The need for significant capital investment in order to make use of the L-GATED solution is just one of the ways that it will attempt to prevent its use for mass surveillance; the others are through operational costs, time delays, oversight, and physical device access. Please see Assumption #8 for further details.

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=

Assumption #16: That operational expense can help restrict the use of the limited governmental access to encrypted devices (L-GATED) solution to only the most exceptional of circumstances.

Why this assumption is reasonable: If the operational expense required to make use of the L-GATED solution is high enough then it will be able to help restrict the use of that solution to only the most exceptional of circumstances. This could be achieved through the use of a substantial computational challenge that would require the use of a highly-capable computational resource that is able to solve the challenge in a reasonable timeframe. The high cost of operating such a resource will naturally restrict the use of this solution to only the most exceptional of circumstances, because not even national governments have unlimited operational budgets. By regularly increasing the computational challenge of the L-GATED solution it will be possible to ensure that its use will always be restricted to such circumstances.

Please note: The high operational cost of the L-GATED solution is just one of the ways that it will attempt to prevent its use for mass surveillance; the others are through capital costs, time delays, oversight, and physical device access. Please see Assumption #8 for further details.

Assumption #17: It is possible to store the master encryption key for an encrypted device, and other related data, in an appropriately secure and tamperproof manner on that device.

Why this assumption is reasonable: The envisioned limited-governmental access to encrypted devices (L-GATED) solution requires that the master encryption key for an encrypted device, and other related data, be stored in an appropriately secure and tamperproof manner on that device. This should be possible by storing such keys, and data, in an Integrated Circuit (IC) that contains non-volatile digital memory, which can only be accessed in a highly secure and controlled manner by the cryptographic systems of the device via a highly-restrictive electronic interface provided by logic that has been hard-coded within the IC, and that any attempt to electronically or physically extract such keys, or data, will be complicated, time consuming and expensive, such that it will be, for all intents and purposes, wholly impractical even in the most exceptional of circumstances.

Please note: By storing encryption keys, and other related data, in a randomly-distributed manner throughout memory locations deep within three-dimensional (stacked) memory it should be possible to make physical access to such memory locations virtually impossible. Only the IC that manages access to such memory will know the exact storage locations. Ideally, this IC would be an Intellectual Property (IP) core within a multi-functional System on a Chip (SoC), which would greatly increase the risks associated with any type of physical tampering, because the encrypted device could easily be rendered completely inoperative if the SoC was even slightly damaged. Attempting to replace a damaged SoC with a new SoC would be pointless because the new SoC would not contain the encryption keys, now irretrievably stored in the original SoC, and which are necessary to decrypt and operate that device.

Assumption #18: It is possible to securely communicate encryption keys ‘related’ to encrypted devices from those devices to a centralized repository.

Why this assumption is reasonable: The envisioned limited-governmental access to encrypted devices (L-GATED) solution requires that encryption keys ‘related’ to encrypted devices be securely communicated from those devices to a centralized repository. Encrypted communications underpin much of the functionality of our modern on-line world, and without such communications many of the on-line services that we currently take for granted would just not be possible. Encryption allows personal and sensitive information to be securely sent over the internet, and has been reliably used for such a purpose for many years. Encrypted communications are now a highly-mature and field-proven technology. Therefore, if encrypted communications are good enough to communicate such things as our personal banking transactions and medical records over the internet then they are also good enough for communicating encryption keys 'related' to encrypted devices from those devices to a centralized repository over the internet, as well. Just because it is encryption keys that are being communicated over an encrypted communications channel, and not banking or medical records, does not suddenly make that channel insecure. Therefore, it should be possible to securely communicate encryption keys 'related' to encrypted devices from those devices to a centralized repository

Please note: Encryption keys 'related' to encrypted devices are just that, keys that are in some way related to those devices. Such keys do not include the master encryption keys for those devices. For more details on this subject please see Stake in the Ground (above). The interception of an encryption key, 'related' to an encrypted device, whilst it was being communicated to the centralized repository, by a bad actor, would not be able to easily compromise the security of that encrypted device, as the bad actor would then require the use of a highly-capable computational resource, which would be prohibitively expensive to own and operate, and be in physical possession of that particular device. Whilst this may be possible in theory, in practice it would require the failure of multiple safeguards built into the L-GATED solution, which would be near impossible. Compromising one device would not compromise any other device.

Assumption #19: It is possible to securely store encryption keys 'related' to encrypted devices in a centralized repository.

Why this assumption is reasonable: The envisioned limited-governmental access to encrypted devices (L-GATED) solution requires that encryption keys 'related' to encrypted devices be securely stored in a centralized repository. There are many data storage systems currently in existence that are able to store data in a highly-secure manner. Such storage systems are often used to store personal and sensitive information, and are often integral parts of mission-critical infrastructures. Such data storage systems are typically housed in physically-secure environments. A similar type of data storage system could, therefore, be used as the basis for the centralized repository of the L-GATED solution. Such a storage system should be able to store the encryption keys 'related' to encrypted devices in an acceptably-secure manner. Therefore, it should be possible to securely store encryption keys 'related' to encrypted devices in a centralized repository.

Please note: Encryption keys 'related' to encrypted devices are just that, keys that are in some way related to those devices. Such keys do not include the master encryption keys for those devices. For more details on this subject please see Stake in the Ground (above)). The theft of an encryption key, 'related' to an encrypted device, from the centralized repository, by a bad actor, would not be able to easily compromise the security of that encrypted device, as the bad actor would then require the use of a highly-capable computational resource, which would be prohibitively expensive to own and operate, and be in physical possession of that particular device. Whilst this may be possible in theory, in practice it would require the failure of multiple safeguards built into the L-GATED solution, which would be near impossible. Compromising one device would not compromise any other device.

Assumption #20: It is possible to appropriately control access to encryption keys 'related' to encrypted devices that have been stored in a centralized repository.

Why this assumption is reasonable: The envisioned limited-governmental access to encrypted devices (L-GATED) solution requires that access to the encryption keys 'related' to encrypted devices, stored in a centralized repository, be appropriately controlled. There are many centralized repositories currently in existence that securely manage the storage of, and access to, personal and sensitive data belonging to thousands, if not millions, of people. Such data can have a wide variety of uses, including banking and stock market trading, and can often be worth millions, if not billions, of dollars. Sophisticated identity and access management systems are used to restrict access to such data to only authorized entities. It should, therefore, be possible to use a similar type of system to appropriately control access to the encryption keys 'related' to encrypted devices that have been stored in the centralized repository of an L-GATED solution. An identity and access management approach for use by an L-GATED solution is briefly discussed in Assumption #7.

Please note: Encryption keys 'related' to encrypted devices are just that, keys that are in some way related to those devices. Such keys do not include the master encryption keys for those devices. For more details on this subject please see Stake in the Ground (above). Failure to stop a bad actor from gaining unauthorized access to an encryption key, 'related' to an encrypted device, stored in the centralized repository, would not allow the security of that encrypted device to be easily compromised, as the bad actor would then require the use of a highly-capable computational resource, which would be prohibitively expensive to own and operate, and be in physical possession of that particular device. Whilst this may be possible in theory, in practice it would require the failure of multiple safeguards built into the L-GATED solution, which would be near impossible. Compromising one device would not compromise any other device.

Assumption #21: It will be possible to turn-off, or destroy, the limited-governmental access to encrypted devices (L-GATED) solution, if required.

Why this assumption is reasonable: It should be possible to devise an L-GATED solution that can be easily turned-off, or destroyed, should it become necessary to do so. In times of threat (to our democratic way of life and our hard-earned civil liberties) the needs of the many (encrypted device owners) must always outweigh the needs of the few or the one (government). The L-GATED solution was devised to solve a very particular problem, and its use for anything else must always be prohibited, even if that means that the solution must be temporarily turned-off or permanently destroyed. So, whilst the operation and the security of the L-GATED solution must be highly robust (bulletproof), it must not be so robust (indestructible) that it cannot be put beyond the reach of any that would seek to abuse it. Whether the L-GATED solution should be turned-off or destroyed is a decision that can only be made by the organization responsible for overseeing its use, and not by any of its users (the national governments of the world).

QyfOjSLUi3I+/sWxBnKu181cvNUz2vsTozh2ogspEbfy8zErOnP32ZXaLovtITLMQZheAI1R8jQ/ByPBEmGCirKBqTteYDs7IVSQyRXupnI=