WHITE PAPER

NSO Group, State-grade Hacking and the Future of Digital Privacy, Security and Freedom for High-profile Law-abiding Persons

Published on: July 28th, 2021

Authored by: Rufo Guerreschi for the Trustless Computing Association and its *spin-out* startup TRUSTLESS.AI.

In this white paper, preceded by a 2-pager Executive Summary, we analyze recent news reports and experts' analysis about the widespread hacking of the smartphones of law-abiding persons. We'll examine why the number of law-abiding persons that are seriously at risk of being continuously and undetectably hacked is ***not in the thousands but in the hundreds of thousands****.*
We then propose a radical mitigation of such problem via a new ***international democratic governance body*** *that will certify end-to-2nd IT systems for digital human communications that radically exceed the state-of-the-art in personal privacy and security, while concurrently ensuring solid international legitimate lawful access. Lastly, we'll examine why that is not only in the best interest of those citizens, and our democracies, but also of powerful western security agencies.*

Executive Summary

Last week, headlines worldwide were raging about a leaked dataset of 50,000 phone numbers that indicated a possible widespread **continuous undetected hacking of the high-profile law-abiding citizens** by governmental clients of the Israeli surveillance company **NSO Group**.

The size of the scandal, and the many uncertainties surrounding it, have brought to the fore the question of **how can we prevent such abuses**, and even more crucially a **wide controversy around how big the problem of such pervasive hacking of smartphones by NSO clients and other entities really is**. Some are claiming it involves only a few thousand victims and others that it extends to hundreds of thousands or even millions.

Apple declared that the "*overwhelming majority*" should not worry, while the CEO of NSO says you should **"*absolutely trust*" in your Android or iOS** phone unless you are a criminal, "*of the Bin Laden kind*". Both have an economic interest in minimizing.

While hard data is hard to get or carefully hidden, Snowden estimated that if the current Wild West market of vulnerabilities - and the inaction of secure smartphone makers - continue, then the number of victims **can soon become 50 million**.

As we argue below, by analyzing what we learned in recent years, one can conclude that the number of law-abiding persons that have a significant risk of being undetectably hacked **can well be in the**

hundreds of thousands or even millions. There are also solid reasons to believe that **wealthy companies and persons may be the majority of those hacked** - for profit instead of for political motive as criminal groups acquire more and more of capabilities of nations, and that **innumerable others can rent those capabilities for a moderate price and minimal risk**.

If the problem is so widespread, **what are the consequences for society?** if we are right, and it is at least in the hundreds of thousands, it is nothing less than a **global emergency for democracy and civil rights** as a few actors with informational superiority are in a position to control, blackmail, extort, and spy on the 99.999% remaining of the people of the World, turning our World into a **Hacker Republic**.

Are there are the solutions to this democratic emergency?

Much has been written these days about **requiring stringent international standards**, such as by Kaye and Schaake, at least among democratic nations, for how these tools are traded, used, and accounted for. Yet, even if that was enacted, enforcement and attribution would be very hard, and restrains on the provisioning of such tools to authoritarian entities **will be replaced by other authoritarian nations and criminal groups**, and our intelligence agencies would lose important visibility they rely on to prevent terrorism and irresponsible nuclear proliferation.

A few others, especially IT security experts have **started questioning if Apple and other smartphone makers are really doing all their best to prevent this hacking**. If with the best technicians and unlimited financial resources Apple cannot there be only one or both of two reasons: (a) a radical minimization of system and supply chains complexity is needed, and/or (b) somehow someone succeeds in making so that those devices are always, at any given time, hackable remotely and undetectably by several powerful nations.

We believe the key solution is to **merge both of these two approaches together via a single new international democratic institution.**

Such a body, launched last month in **Geneva**, and called Trustless Computing Certification Body (TCCB), will **certify that given IT systems dedicated to sensitive human communications ensure both levels of security and privacy radically higher than state-of-the-art, and concurrently ensuring international legitimate lawful access**.

Such a body will offer all nations to state their case for any need for lawful access request, **on a voluntary basis** as no legal mandate exist. Such requests are vetted by a jury-like body of citizens, for local requests, or by a committee of former international judges, for international requests by nations participating in the governance of the body. Those subject to a **highly democratic, competent and resilient international governance** structure and statute of such body. All this without changing a single law.

If we have stirred your interest so far ;-) then book some time, to read our detailed analysis and case below in this white paper.

We'll analyze all this in steps, in this white paper. We'll start by analyzing the recent "NSO 50k Affair", to then deeply analyze if this is a problem for a few thousand people or for hundreds of thousands. We'll then look at a proposed solution, and analyze how it **breaks away from the zero-sum game**

downwards spiral to realize a wide-ranging win-win solution that advances both civil liberties and public safety, just like we did with the social contracts we conceived and implemented when we created our democratic constitutions in the pre-digital era.

1. The NSO 50k Affair

Last week, the leading Israeli spyware company NSO Group was for several days on top of the headlines around the World. Seventeen leading World news organizations presented the results of a year-long joint investigation around **a dataset of 50,000 phone numbers**, of yet unknown origin, which allegedly lists persons "targeted" for hacking worldwide by about 20 governmental clients of the NSO Group.

Hundreds of journalists, parliamentarians, activists, 12 heads of state, and directors of major media organizations were included. A forensic analysis by Amnesty International and Citizen Lab of a few dozen of the smartphones 9o to those numbers found that **half of them were hacked**, or attempted to be hacked.

Much is still unclear and may remain so, since we are deep into spy territory. What is the source and origin of the dataset? How many of those 50,000 on the list were hacked? How many were attempted to be hacked? Was that list, instead, a sort of full or partial "wish list" of NSO governmental clients, most of which were eventually turned down *ex-post* by NSO and/or via vetting processes by Israeli authorities? And many other key questions linger on.

Regardless of these unanswered questions, most media outlets jumped to the **early conclusions** in headlines and also in articles that those 50,000 persons were all hacked, or attempted to be hacked.

Also, NSO Group was depicted as an evil entity, and the only company doing this, while the **crucial role they and similar entities in preventing international terrorism to dangerous nuclear proliferation** were nearly completely ignored, in a shameful lack of gratefulness.

2. A Dangerous World

Unfortunately, we live in an **increasingly dangerous world**, full of divisions, blind doctrinal beliefs, deep-seated hatred, and large-scale disinformation that lead many of our fellow humans to violence, terrorism, war, and subversion of democracy.

While over 30% of Americans believe the Presidential elections were stolen, we know there are over 30 million ISIS sympathizers in Arab countries.

Meanwhile, **a recreational drone can easily be weaponized** with information available on the Internet to spread chemical, radioactive, or biological agents to kill millions. IT and AI-driven innovations in all sectors are lowering the resources needed to weaponize technologies to cuase huge harm.

Yet, the need to prevent the bad guys has spurred the creation of **regimes of pervasive private and state surveillance,** that have nearly eliminated civil rights, accrue huge power of

manipulation of public consent in a few hands, and are fast **eroding democracy** itself, at home and abroad, contributing to a slide towards authoritarianism in a feedback loop.

3. A Crisis of Informational Superiority and Democracy

The laws and programs our western nations have enacted **to prevent terrorists and rogue nations from abusing encryption** to commit grave crimes have created a **huge asymmetry in informational superiority** that is fast widening at an accelerated pace.

On one side, **a few dozens of tech ultra-billionaires and nation-state elites** can protect their information and spy on the information of others.

On the other side, **the remaining 99.999% of us**, including millions of journalists, elected officials, politicians, activists, wealthy businessmen, and their associates, who have nowhere to hide and **we are hacked via powerful AI in social media feeds** into buying not just their products, but their idea and candidates, and fake news.

This widening informational asymmetry translates into an **equivalent financial, power, and political asymmetry** that not only creates huge disparities of wealth, prevents to further reducing poverty and sickness but, even most importantly, prevents humanity from coming **together as free human beings to rationally and democratically** tackle the unprecedented challenges and opportunities facing it in the years to come.

4. Awareness and Sizing the Problem

The NSO 50k affair has led journalists and analysts to re-analyze the revelations of news of recent years about how vulnerable **even the most sensitive law-abiding persons in society** are to devastating and extended abuses of their privacy, at the hand of participants in a billion-dollar shady market of hacking tools made of nations, criminals, researchers and state-regulated companies like NSO.

Many have started realizing that the root problem is that **even the most secure smartphones out there** are by far not as secure as they were believed to be, how they should be, or how they could be, while secure messaging **apps cannot be more secure than the device they run on**.

Yes, huge questions have still gone unanswered: **Who has a substantial risk of being hacked? Is it a few thousands, or is it hundreds of thousands, or millions?**

Which are the most targeted demographics?

5. Who and How Many are at Risk? NSO and Apple answer

Both NSO and Apple rushed to minimize the scope of the problems, which aligns with their direct economic and reputational interests.

Apple declared a few days back: "*Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals. While that*

means they are not a threat to the overwhelming majority of our users, we continue to work tirelessly to defend all our customers, and we are constantly adding new protections for their devices and data."

Their use of the term "*overwhelming*" is compatible with **millions of devices hacked**, which would amount to 0.1% of the 1.5 billion iPhones out there. Yes, those tools "*cost millions of dollars*" to develop by are then sold and used by many, and sometimes stolen or leaked. They state that iPhone exploits "*often have a short shelf life*", admitting how there are some critical vulnerabilities, as widely reported, that have not been fixed even though they have been (inexplicably?) exploited at scale by powerful governments (and others?) for years. They, also state that they "*continue to work tirelessly to defend all our customers, and we are constantly adding new protections for their devices and data*" but, if they do, and year on year the weaknesses do not improve, how much can we trust that they are trying hard enough?

Meanwhile, NSO Group CEO Hulio declared: "*The people that are not criminals, not the Bin Ladens of the world—there's nothing to be afraid of. They can absolutely trust the security and privacy of their Google and Apple devices.*". These statements comment themselves after what we have learned. Of course, you don't need to be Bin Laden to be illegitimately intercepted by NSO clients or other entities. Of course, suggesting that all those that are not criminals (of the Bin Laden kind) should have "absolute trust" in their Google and Apple devices is a wild and irresponsible statement after what we have learned in these years.

Security agencies also have a huge interest to minimize, because **if most or all criminals knew how hackable their IT was they would not abuse them, and get busted**. That is why the FBI (most likely) staged an act for months pretending not to be able to open an iPhone when there were several companies and researchers (but not the NSA?) able to do so.

6. Who and How Many are at Risk? What is the cost of attacking a given person? Are you at risk? Let's see.

There is no way to quantify precisely how many have a high chance to be singled out for such hacking, but many bits of evidence support the case that **millions or tens of millions of high-profile individuals** may be currently hacked, or potentially hacked any day, or in the near future as estimated by Edward Snowden, if this way of things continues.

That includes over 100,000 elected **parliamentarians** and national **politicians** around the World, tens of thousands of front-line **journalists** and **activists** - and their close associates - hacked for political motives. But also hundreds of thousands of executive and wealthy individuals, and their close associates, targeted primarily for profit motives.

Although NSO tends to stay on the leading-edge, similar capabilities are offered by many **other companies** and are available independently to several powerful nations.

Given technical and "political" limitations of NSO Group tools, clients purchase systems, and services from **multiple vendors from other countries**, even 20 at once in some cases, to hack targets in their wish list that are blocked by one provider and to leverage advantages that some tools may have on certain target IT systems at a given time.

Major known **vendors are from Germany, France, US, and Italy**. It is also likely that many nations acquire similar tools from nations like Russia and China. Also, many nations, several different agencies have separate contracts with the same provider.

In addition, many **governments that are clients of hacking tools** also often invest greatly to build their one tools and capabilities, hiring dozens of expensive mercenary hackers, and sometimes top former western operatives, and rely on **a billion-dollar black market of exploits** and hacking systems made up of brokers, ethical researchers, and criminals.

There are another **170 nations that have not been mentioned** in this recent NSO scandal, many of which can be expected to operate similarly, purchasing tools from other vendors, and developing their own capabilities.

A **phone number is often all it takes** to take full control undetectably for months and years of the victim's phone. Most hacks happen remotely via messages from sources apparently known or trustworthy to the victims, or via **no-click messages on iMessage or WhatsApp**. Some are quickly fixed while others, while some (unexplainably?) remain exploitable for years. Hacks of Android devices often leave no traces even to forensic of the most advanced labs in the World.

The need of the nations of origin of the hacking system providers to limit who gets hacked (NSO excludes number from the US or temporarily in the US), the difficulty of ex-post security audit of such systems, and the ease of hiding one's tracks in today's IT, often **allow intelligence agencies to "piggyback" on systems like NSO Pegasus to spy on those such clients spy on**.

Even more concerning, those or similar capabilities are available to **dozens or hundreds of criminal groups**, more or less connected to a state, that autonomously develop such tools or come in their possession via leaks like Vault 7 and like Shadow Brokers, or even entire infrastructures such as via the Hacking Team hack - and most concerning of all **innumerable others that can "rent" their capabilities at moderate cost and minimal risk**.

Furthermore, the lawsuit that Facebook has against NSO provides details and proofs of 1400 WhatsApp hacked in the course of 2 weeks (!). This means **35.000 persons whose phone was completely taken over by NSO tools over one year.**

The hacking by NSO clients is **overwhelmingly driven by political motives** to maintain the current elected government or regime in power, by stifling, discrediting and anticipating the actions of dissents, critics, and opposition, and blackmailing them by spying on their relative wrongdoings or socially questionable practices.

Yet, a similarly huge problem is criminals have only a profit motive and so, therefore, tend to use such tools for extortion, ransomware, blackmail, and financial fraud **attacks on the World's wealthiest individuals and firms**. They may do so autonomously or be hired by brokers on behalf of other less technical criminals, competitors, adversaries, former family members, or employees.

How much does it cost in money and risk to attack a single person?

There is much confusion as we read the news that a hacking tool (exploit) for **the iPhone can cost up to $1-2 million on the Dark Web**. But the truth is that the costs and risks for an adversary to

hack pretty much anyone - except a few chosen ones that received special crypto devices (supposedly safer) from nations states - is very low because many of those tools scale quite well. Yes, some of them get regularly burned from overuse, but other ones stay on for years (how come?), and fresh ones are found all the time by a shady billion dollars industry of nations, firms, criminals, and researchers.

Although NSO's Pegasus is the Roll Royce of hacking tools, t costs **about $10,000 dollar for undetectably hacking continually any target user**, as reported by the New York Times in 2018: "*NSO Group charged $500,000 to set a client up with the Pegasus system, and then charged an additional fee to actually infiltrate people's phones. At the time, the costs were reportedly $650,000 to hack 10 iPhone or Android users, or $500,000 to infiltrate five BlackBerry users. Clients could then pay more to target additional users, saving as they spy with bulk discounts:* ***$800,000 for an additional 100 phones,*** *$500,000 for an extra 50 phones, and so on. NSO would also reportedly charge 17 percent of what the clients had paid over the course of a year as an annual maintenance fee. According to Forbidden Stories, NSO's contract with Saudi Arabia alone is worth up to $55 million".*

Ok, but then **how can the dozens of powerful state and criminal entities that have these capabilities operationally hack and manage hundreds or thousands of devices and persons while minimizing discovery**? Well, already ten years ago powerful national agencies like the NSA had capabilities to turn targeted surveillance into a scalable enterprise via systems and programs like NSA FoxAcid, NSA Turbine, and similar functionality offered (or at least marketed) by private equivalents like the Italian Hacking Team RCS. Ten years later we can well expect that more advanced AI and algorithms are even more effective at making targeted hacking completely automated or semi-automated at scale.

In light of what we've learned, the lofty claims of security by companies like Apple, Signal, sound very allow and less than genuine. Meanwhile, the **self-defense guides by associations like EFF, ACLU, or The Intercept may have been unwittingly but tragically misguided**, placing many many activists and journalists in very danger over these years, by overestimating, still today, substantially the protection offered by the best tools or the most elaborate precautions.

Security agencies are happy to play along in supporting the overestimation of the security of current secure IT, so as to be able to intercept them as needed and be able to cry for "going dark" once in a while to make sure their capabilities are not diminished by new laws.

7. Why this widespread Hacking is our Worst threat to Democracy

Given the huge scale of this hacking, this state of affairs has **huge costs** for the targeted individuals and for society-at-large. For those individuals, there is a huge loss of civil rights, freedoms, frauds, and risk for bodily harm. For our society-at-large, there is a huge cost in terms of **democratic sovereignty**, freedom of the **press**, and freedom of **assembly**.

Even worse, as the *UN High Commissioner for Human Rights Michelle Bachelet* argues, this leads to **self-censorship**, whereby all need to assume that excerpts of any of their communications could be used by an adversary for evil purposes. And even more after these revelations.

The dilemma at the root of the NSO 50k Affair is indeed very hard to solve, and getting harder: **how can we concurrently satisfy the two crucial and vital needs of (a) affirming civil rights in cyberspace while (b) preventing very grave crimes through abuse of encryption?**

8. Why are we in this situation?

To solve the problem we first need to understand how we got here.

The root problem is that we live in a semi-anarchic World - one without any sane collective democratic governance - where **dangerous technologies, people, and nations abound**. Fortunately, some nations have taken on themselves the responsibility to protect themselves and the rest of the World against those huge global risks that can easily lead to large-scale loss of life, conflict, and threats to democratic institutions.

To protect our safety, **nations have had a vested interest in inserting, letting in, and managing subtle weaknesses in all secure IT and IT security standards** used for human communications, in a plausibly deniable way, to ensure access for themselves at all times.

To date, the need for public safety has prevailed, so nations have proceeded to ensure that no one in the World, except authorized officials, can access IT that enables them to escape surveillance if that is legally authorized. That has served their cyber-investigation capability very well.

Yet, the collateral damage has been enormous. In fact, we also live in a World **sliding towards authoritarianism**, where widespread privacy abuses by authoritarian governments of dissidents, journalists, opposition figures, and their associates, has become a more and more **decisive instrument for the long-term entrenching of their authoritarian power**, as we've seen happen especially in China, but much also elsewhere, and pretty much everywhere, really.

So, therefore, safeguarding the safety, democracy, and civil rights within our western nations, and internationally, requires **both the enablement of cyber-investigation capability and protection from privacy abuse from state and non-state**.

Somehow, secure IT providers like **Apple**, even with nearly infinite R&D resources, always end up with their devices, like the iPhone, somehow (??!!) always short of being hackable at scale, at any given time, by at least a number of large nation-states.

How come when there is a huge demand for higher levels of security, when **family offices and high net-worth individuals**, accruing $60 trillion in assets, see cybersecurity as their n.1 and their n.2 concerns?

So, it may very well not be an accident. In fact, we are really good at security and safety engineering and standards, as **only 1 out of 16 million commercial flights result in an accident**. Meanwhile, 1.5 billion phones are made every year, each hackable by innumerable actors. The truth is all IT because **safety trumps privacy when given a stark choice,** in the mind of both governments and the people that elect them.

There can be only 2 rational explanations or a mix of the two.

One, it could be that the increasing **hyper-complexity of their systems and supply chain** needed to offer even faster and richer user experience and entertainment, to keep us glued to such devices, is incompatible with achieving high-enough security.

Two, it could be a deliberate activity by Apple and/or some of its employees, to leave in critical bugs that are discovered during development or internal testing (so-called "**bug-doors**"), and share those with governments, in plausibly deniable ways, or just let them find them.

In fact, the two requirements go along well: being able to push complexity beyond what would be rational to maintain the target security levels, enables Apple and its competitors to offer a richer and richer experience, at the expense of our freedoms, as we've seen.

9. Is there a solution to this "NSO 50% dilemma"?

The dilemma at the root of the NSO affair is indeed very hard to solve, and getting harder: **how can we concurrently satisfy the vital need to affirm civil rights in cyberspace, and the vital need to prevent grave crimes through abuse of encryption?**

At the Trustless Computing Association and its spin-out startup TRUSTLESS.AI, are building a new Swiss-based ultra-resilient international **democratic** governance body that will certify IT systems for digital human communications that will **radically** exceed state-of-the-art in privacy, security, and democratic control, while **concurrently** ensuring international *legitimate* lawful access, by **applying to both** extreme battle-tested socio-technical safeguards, the Trustless Computing Paradigms.

Such *Trustless Computing Paradigms* include, among others, these unique requirements for a compliant IT service: (a) **transparency** of the source designs of the critical hardware and software components; (b) extreme level of "ethically-aligned" security **review in relation to complexity**; (3) wide utilization of **citizen-witness and citizen-jury** mechanisms within the lifecycle; (4) inclusion of the presumable motives of key staff, executive and shareholders, as a key element of trustworthiness.

We use the word "**radically**" as the best quantitative approximation of the target security levels of TCCB, whereby perfect security will never exist, and incremental improvements are useless to the user given how low the current bar is.

Last June 24-25th, during the 8th edition of Free and Safe in Cyberspace conference series in **Geneva**/online, we formally and finalized and established the Trustless Computing Certification Body (or "TCCB"), with World-class partners, advisors, and speakers, including top IT security experts, former top cyber diplomats from leading nations, and executives of top EU banks.

Meanwhile, the startup spin-out is building the 1st TCCB-compliant open target architecture, open computing base, and end-end IT system. It is building a TCCB-compliant private cloud and a **standalone 2mm-thin personal computer** - embedded in a custom leather wallet or in the back of smartphones of all price levels.

While being a **stand-alone** personal computer, it **seamlessly complements your smartphone** for Internet connection, data transfers, and 2-way multi-factor authentication.

Governance is absolutely central to the aims of the TCCB. Governance is "where the buck stops": the ultimate point of failure and the source of all present and future trustworthiness, actual and perceived, of TCCB-certified IT services. Its governance and statutes are thus conceived with the utmost care to maximize the likelihood it will sustainably remain **highly citizens-accountable, technically proficient, effective, altruistic, and resilient** to undue processes from powerful state and non-state actors.

10. Is TCCB really in the interest of powerful nation-states?

The wide adoption of TCCB, we believe, would be in the best overall interest of powerful western nations, like the US and Israel, and even just in the narrower interest of their security agencies.

Although the TCCB can be governed with suitable global accountability, competence, and resiliency without asking any government permission, or any legislative change, and without the participation in the governance of a balanced mix of nations, the latest is highly desirable and to reinforce its actual and perceived democratic accountability.

TCCB will enact **battle-proven and novel socio-technical safeguards** - down to the hardware fabrication - to ensure both ultra-high levels of user security and privacy AND the resilience of a procedural in-person "front-door" mechanism, involving highly resilient and **representative international judges and citizen-jury processes**.

TCCB will commit to evaluating cyber-investigation requests submitted by participating nations in return for their binding commitment to **disclose** to TCCB, and only to it, the vulnerabilities they find in those systems.

Participating nations could increase the **availability of much more trustworthy IT for their most sensitive systems for human communications and transactions, public and private while retaining their ability to access when there is a *legitimate* need or mandate.**

Participating nations would also **enable their politicians, journalists, activists, and elected officials, with the utmost protection against all attackers, foreign and domestic, to protect national sovereignty and democracy**.

Participating nations could eventually extend those certifications as preferred or mandatory for the **critical subsystems** of the most sensitive public and private systems - such as electoral systems, critical infrastructure, and dominant social media platforms - to further protect democracy, safety, and national security.

Yes, in a scenario of the wide roll-out of TCCB, powerful participating nations would lose their arbitrary ability to hack into such IT systems. Yet, arguably, their cyber-investigation capability would overall improve.

In fact, currently, **targeted state endpoint hacking has substantial issues of consistency and often produces untrustworthy evidence and intelligence,** due to several reasons: target devices are updated providing temporary “going dard” problems; there is a high probability of concurrent undetected hacking by multiple entities on the same device - and the fact that such systems are often designed to make forensic analysis harder rather than easier In fact, evidence so acquired via

state trojan is structurally contested by highest civilian courts in Germany and France, as well as in Italy.

As highlighted by Rami Efrati, former Head of Cyber Division of the Prime Minister Office of Israel, during a recent university lecture (min 9.35), intelligence agencies' legitimate hacking capability is often inconsistent, as a consequence of the fact that all IT end-points are broken at multiple levels.

With TCCB, instead, cyber-investigation requests by participating nations for such IT systems would be **ensured to produce the data of a legitimate suspect or criminal in a timely manner**, and produce evidence that is much more attributable and, therefore, to stand as valid evidence in the highest courts. Lawful access requests could be processed within 1-2 hours, in urgent cases.

In addition, all end-users of a TCCB-compliant system will need to undergo **state-of-the-art background checks and KYC** (know-your-customer), and very strong initial biometric authentication, reducing further the risk of abuse.

11. How will it work if a nation submits a lawful access request?

As detailed in our TCCB Cloud, an integral part of the Trustless Computing Paradigms:

"Nations that choose to join the TCCB governance, with its benefits and obligations - and nations where a TCCB-certified Cloud locates one of its hosting rooms - are guaranteed the ability to submit a lawful access request to the TCCB or to a local TCCB Provider, which will be handled according to the TCCB Cloud process, which is summarized here below:

1. *If the access request is by the **national** government (meaning one where one of the three redundant hosting rooms of the TCCB Cloud is located) - or by a foreign government, whose access request is appropriated by such government - then such request will be:*
    1. *vetted in their due process (not in the evidence) by a **TCCB Jury**, a jury made of 5 or more random-sampled citizens of such national government and 2 random-sampled parliamentarians of local national jurisdiction, which will act as both citizen-jury and citizen-witnesses. Every 3 months, 15 are sampled and instructed. When the need arises, 10 are randomly called, as soon as 5 arrive, the process can begin.*
    2. *If the request is approved by the TCCB Jury, the Jury proceeds to physically provide access to the request data and/or keys of a specific user, according to the approved part of the request.*
2. *If the access request is by a **foreign** government, then such request will be:*
    1. *vetted by a **TCCB Judicial Board**, made of 15 recognized experts in international law, civil rights, and public security, who have been elected or appointed to high offices, such as a leading international court, the highest court of a large democratic nation. Deliberation will happen remotely using TCCB-compliant devices to provide the utmost confidentiality safeguard of the evidence being analyzed. The Board decision will assess the "legitimacy" for each request by evaluating the furnished and autonomously-acquired evidence to determine to what extent the request complies with the national legislation where TCCB is based (Switzerland currently), and it maximizes:*
        1. *Compliance with and promotion of international civil rights and civil rights norms.*

    2. *Promotion of international security and safety.*
    3. *Compliance with laws and constitutions of the jurisdiction of the requester and the target.*
2. *If the request is approved in full or in part by the TCCB Judicial Board, then the TCCB Jury will be instructed and ordered to allow access to specific users' data and/or keys according to the approved part of the request."*

12. Dealing with Geo-political and National Security requirements

Often **powerful nations "piggyback" (ie. "hack into") surveillance tools and programs** used by other nations - including those sold by their own state-regulated companies - in order to acquire valuable intelligence while further minimizing the risk of being discovered and maximizing plausible deniability. This activity has genuine value for promoting national and international security but, as we've seen, creates huge problems for civil rights and democratic accountability.

Should TCCB-complaint IT systems be made widely available in countries with a high concentration of radicalized persons, and led by unreliable governments, powerful western nations like Israel, US, and Germany, could lose some of the leverage and control they currently hold towards governments intelligence apparatus through the provisioning of hacking tools, which is important to promote pressing national and international security needs.

But that can be mitigated in several ways. **The traditional leverage gained by selling them hacking tools could be replaced by selling ultra-secure IT that is TCCB-compliant**, and beyond, that enables them to be protected from anyone spying on them, except when the international *TCCB Judicial Board* decides a legitimate investigation is warranted.

By selling TCCB-compliant IT systems in the private and governmental markets, TCCB participating nations and their state-regulated cyber champions can take a lead in the global market of cybersecurity, secure communications, and other markets where cybersecurity will be a key competitive advantage, like advanced AI and autonomous systems.

Israel itself could make up lost business from NSO by several orders of magnitude, by being best positioned in a leadership position considering that 41% of global cybersecurity investments are in Israeli companies, as reported this week by Israel's new Prime Minister Naftali Bennett.

In fact, the **uniquely transparent and trustworthy security assessment** process of TCCB, and radically mitigating the actual and perceived risk of "bug-doors" or backdoors in IT systems, which has substantially limited the market of their IT in sensitive domains, and create a very distinct objective competitive advantage versus highly competitive but autocratic competitors, like China.

TCCB **early** participating nations could then acquire an early innovation and economic advantage in a crucial market and domains, promote a **renewed cyber soft power** to increase their geopolitical dominance while **making civil rights and democracy stronger**, and the World more secure and safe.

In line with this vision, Jake Sullivan, Biden's appointed US National Security Adviser stated last month that **new true global soft-power leadership in security, privacy and democratic social**

networks - and not just in words and rhetoric, but in objective solid and transparent standards, could even be key to leadership in the AI race with China.

On the same line, the US National Security Commission on Artificial Intelligence reports: "*The United States can use diplomacy and leverage its global partnerships to advocate for establishing privacy-protecting technical standards and norms in international bodies, and it can work with like-minded nations to ensure that other nations have an alternative to embracing China's technology and methods of social control and access to technologies that protect democratic values like privacy*".

13. From TCCB towards Cyber Peace

Since TCCB certifications will also require much higher levels of **forensic-friendliness** - participating nations would benefit from much improved - and internationally and objectively provable - cyber attribution capability for cyber incidents involving TCCB-compliant systems.

As a resulting benefit, as the number of participating nations increases and more of their critical systems are TCCB certified - those nations would realistically be able to engage in **enforceable cyber treaties** and/or in **fair and responsible retribution** for grave violations of international norms, contributing substantially to cyber peace and therefore World peace.