Five Ways to Prepare for the Online Privacy Crackdown

5 Ways to Prepare for the Online Privacy Crackdown

> ***With legislation around the world seeking to gut encryption and online anonymity, Ramiro Romani offers an overview of what's coming and several solutions for divesting from Big Tech products and protecting your online privacy.***

by **Ramiro Romani**, *Unlimited Hangout*
November 6, 2023

The internet is about to change. In many countries, there's currently a coordinated legislative push to effectively outlaw encryption of user uploaded content under the guise of protecting children. This means websites or internet services (messaging apps, email, etc.) could be held criminally or civilly liable if someone used it to upload abusive material. If these bills become law, people like myself who help supply private communication services could be penalized or put into prison for simply protecting the privacy of our users. In fact, anyone who runs a website with user-uploaded content could be punished the same way. In today's article, I'll show you why these bills not only fail at protecting children, but also put the internet as we know it in jeopardy, as well as why we should question the organizations behind the push.

Let's quickly recap some of the legislation.

European Union

– Chat Control: would require internet services (Email, chat, storage) to scan all messages and content and report flagged content to the EU. This would require that every internet based service scans everything uploaded to it, even if it's end-to-end encrypted. Content would be analyzed using machine learning (i.e. AI) and matches would automatically be reported to the police. This is awaiting a vote from the EU LIBE committee.

United Kingdom

–The Online Safety Act 2023: would require user service providers to enforce age limits and checks, remove legal but harmful content for children, and require scanning photos for materials related to child sexual abuse & exploitation, as well as terrorism. It would require providers to be able to identify these types of materials in private communications and to take down that content. This means providers would need visibility into messaging, even those messages are end-to-end encrypted. End to end encrypted messaging providers such as WhatsApp, Viber, Signal, and Element have indicated in an open letter that surveillance on of this type simply isn't possible without breaking end to end encryption entirely, and have threatened to leave the UK if the bill was passed & enforced without the offending Clause 122. This bill was recently passed by parliament unchanged and will become enforceable in 2024.

United States

– The EARN IT Act 2023: would allow US states to hold websites criminally liable for not scanning user uploaded content for CSAM (child sexual abuse material). This would effectively ban end to end encryption. This bill has 22 cosponsors and is awaiting an order to report to the Senate.

– The STOP CSAM Act 2023 (Full Text): would allow victims who suffered abuse or exploitation as children to sue any website that hosted pictures of the exploitation or abuse "recklessly", e.g. if your website was not automatically scanning uploads. Websites are already required by law to remove CSAM if made aware of it, but this would require providers to scan all files uploaded. This bill has 4 cosponsors, and is awaiting an order to report to the Senate.

– Kids Online Safety Act (KOSA): would require platforms to verify the ages of its visitors and filter content promoting self-harm, suicide, eating disorders, and sexual exploitation. This would inherently require an age verification system for all users and transparency into content algorithms, including data sharing with third parties. This bill has 47 bi-partisan cosponsors and is awaiting an order to report to the Senate.

Its important to note that the language in these bills and the definition for "service providers" extends to any website or online property that has user-uploaded content. This could be as simple as a blog that allows comments, or a site that allows file uploads. It could be a message board or chatroom, literally anything on the internet that has two-way communication. Most websites are operated by everyday people – not huge tech companies. They have neither the resources or ability to implement scanning on their websites under threat of fine or imprisonment. They would risk operating in violation or be forced to shut down their website. This means your favorite independent media site, hobbyist forum, or random message board could disappear. These bills would crumble the internet as we know it and centralize it further for the benefit of Big Tech who are rapidly expanding the surveillance agenda.

We must pause and ask ourselves, is this effort to ramp up surveillance *really* about protecting children?

How do companies currently deal with CSAM?

In the United States, tracking CSAM is recognized as a joint effort between ESPs (Electronic Service Providers) like Google, and the National Center for Missing & Exploited Children (NCMEC) a private non-profit established by Congress in 1984 and primarily funded by the United States Department of Justice. *Unlimited Hangout* has previously reported on the NCMEC and its ties to figures such as Hillary Clinton and intelligence-funded NGOs such as Thorn. They also receive corporate contributions from big names such as Adobe, Disney, Google, Meta, Microsoft, Palantir, Ring Doorbell, Verizon, and Zoom.

Ashton Kutcher's NGO Supplies Police with 'Free' CIA-linked Surveillance Tool to 'Protect Kids'

Electronic service providers in the United States are already required to report to the CyberTipline (Federal statute 18 USC 2258A) if they become aware of CSAM, otherwise they may face fines or prison time. These CyberTipline reports combine offending content with additional information such as identifying the potential perpetrator, the victim, and other context that is combined and sent off to law enforcement.

Photo & content scanning measures are not required. However, several prominent companies have voluntarily implemented scanning of communications and media, such as Gmail, YouTube, Google Photos, Facebook, Instagram Messenger, Skype, Snapchat, iCloud email, and Microsoft's Xbox. If you use these services, then your messages and media may automatically be scanned for abusive material.

Ironically and not surprisingly, its these very platforms that have the most malicious activity, including drug & guns sales, child abuse material, and cyberbullying/harassment.

Does voluntary content scanning actually help protect children?

Google began publishing a CSAM transparency report in 2021 which gives numbers on how much CSAM was identified and reported on across Google & Youtube. It includes data since 2020, with counts for how many reports were made to the NCMEC, how many different Google accounts were disabled, and how many “hashes” (photo fingerprints) were contributed to the NCMEC hash database.

It is unclear exactly when Google started creating “hashes” of its users photos, but they have contributed 2.5 million new hashes to National Center for Missing and Exploited Children’s Hash Database to date. Reports are published every 6 months, and we’ve seen staggering growth in all types of reports since 2020. For example, Google’s CyberTipline reports have grown from ~547,000 in 2020, ~870,000 in 2021, to more than 2.1 million reports in 2022. The first half of 2023 has shown a decline, totaling ~750,000 reports from January to June.

As seen on NCMEC’s CyberTipline Data page, Google’s reports represent a mere fraction of the total number of reports submitted to the NCMEC, which works with over 1,500 ESPs – mostly US companies. 5 electronic service providers (Facebook, Instagram, Google, WhatsApp, and Omegle) accounted for more than 90% of the 32 million reports in 2022. Around half (49%) of these reports in 2022 are “actionable”, meaning there is sufficient information for law enforcement to proceed with an investigation. Additionally, 89.9% of reports involved content uploaded by users outside of the US.

The NCMEC also reports the numbers of CyberTipline reports made to different law enforcement organizations such as Internet Crimes Against Children, Local LE, Federal LE, and International LE.

Law enforcement is not required to give any feedback on what happens with these reports and, as a result, they hardly provide feedback. Using the NCMEC’s own numbers, we can see there is little visibility on how the reports are used.

In 2022, we saw the following rates of feedback from law enforcement and other groups who received reports.

- International Crimes Against Children Groups – 491,655 actionable reports resulted in 41.59% Feedback

- Local Law Enforcement – 1,462 actionable reports resulted in 3.48% Feedback
- Federal Law Enforcement – 1,356,988 reports resulted in 0.03% Feedback
- International Law Enforcement – 13,995,567 reports resulted in 0.4% Feedback

Keep in mind, a feedback response doesn't necessarily mean an arrest or conviction. Feedback responses could may indicate the report was closed or incomplete feedback. Also, these results are not open to the public, although a FOIA request could change that. However, these numbers make it clear that whether companies are voluntarily scanning their content or creating reports after becoming aware of CSAM – there's no visibility on what actually happens with the reports.

Given the huge volume of reports not acted upon, forcing technology providers to automatically scan content & generate reports is not going to magically change things. It will require law enforcement to act on reports to put child predators behind bars and save children. That is, after all, what legislators say they want.

That's not to say nothing is being done. A 2022 report of CyberTipline success stories in the United States stated that close to 714 different cases used CyberTipline reports. Only 16 of these cases explicitly reported the assistance of a service provider.

Again, out of 1.35 million actionable CyberTipline reports in the United States in 2022, there have been 714 arrests so far. Its possible there are ongoing investigations that will bring this number higher, but we can only guess without transparency. I was unable to find success stories for any prior years.

I commend these efforts to protect children from dangerous predators; however, these efforts do not necessitate automatic scanning of everyone's messages or the gutting of encryption. Generating more reports from service providers obviously does not lead to more arrests being made. Lastly, the majority of CSAM material comes from big tech providers, many of whom are voluntarily scanning content anyways. Why enforce this requirement on every website on the internet?

If legislators around the world want to make a genuine impact on child abuse, then they should push for transparency and accountability practices for law enforcement and work to ensure that law enforcement properly investigates the millions upon millions of reports they already receive every year, and make the data available to the public.

We the people need to know that the groups responsible for investigating child abuse are doing their jobs with the processes and data already available, rather than further sacrifice our individual privacy and security for more of the same. The bills/laws in question also lack an understanding of encryption, are not technically feasible to implement, put unnecessary legal liability on technology companies, and lack evidence that the policies will improve outcomes for children.

How can the online child abuse laws across Western countries be so consistent with their practices? How did they all reach the same strategies of age verification, content filtering, and client side scanning?

The framework for this legislation has been in the works for years. One key architect of this push has been the WePROTECT Global Alliance, a merger of initiatives between the European Commission, the US Department of Justice, and the UK Government. Their first summit was hosted in 2014 and is now comprised of 97 governments, 25 technology companies, and 30 civil society organizations.

UNICEF, a member of WePROTECT, released a "model national response" which outlines many of the elements we see in these different child safety bills today. UNICEF and organizations like the US Department of Justice state that sexual exploitation of children cannot be addressed by one country, company, or organization working in isolation. Troublingly, both of those groups have a history of turning a blind eye to child abuse in their respective organizations and/or jurisdictions (see here, here, here and here for examples).

Working groups like the "Five Country" government counterparts (Five Eyes) – USA, UK, Australia, Canada, New Zealand– have met with the corporate executives of Facebook, Google, Microsoft, Roblox, Snap, and Twitter to collaborate on guidelines such as the "Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse" (justice.gov link). These groups are all working together, via public-private partnerships like the Global Cyber Alliance, among others, to change the face of the internet.

Earlier this year, the Department of Justice outlined the "risky" aspects of technology in a 2023 National Strategy Report on Child Exploitation:

> *– an uneven response to online child safety by the tech sector;*
> *– a CyberTipline system that is overwhelmed;*
> *– anonymization of offenders;*
> *– encryption of data storage and communications;*
> *– online environments where children and adults interact without supervision or controls;*
> *– globalized, often sovereignless, platforms;*
> *– remote, often extraterritorial, storage; and*
> *– a compounding lack of public awareness of these risks.*

While the issue of child exploitation online is grave and child abusers need to be held accountable – this shouldn't come of our individual privacy and freedom. From the publicly stated perspectives of these groups, anonymization, encryption, and not allowing governments or tech companies to track all content is equivalent to contributing to child exploitation.

Ignoring the child abuse right in front of their noses

As noted earlier, many of these groups have a track record of responding very poorly to serious child abuse issues when these crimes involve their own organization or persons with political value. For instance, there have been nearly 2,000 allegations of child sexual abuse and exploitations made against U.N “Peacekeepers” worldwide between 2004 and 2016, as reported by the *Associated Press*. This includes the child sex ring in Haiti from 2004 to 2007 where Sri Lankan UN “Peacekeepers” traded food in exchange for sex with children as young as nine years old.

The names of the offenders are kept confidential by the UN, and the UN puts the responsibility on member states to investigate & prosecute. UN records on these allegations are also incomplete and hundreds of cases have been closed without explanation. The United Nations even continues to send Sri Lankan peacekeepers to Haiti, despite the scandals. In the United States, we can see a similar level of accountability with the Department of Justice still withholding the client list for Jeffrey Epstein’s child prostitution ring, among many, many other examples.

The very organizations that try to convince us to give up our individual liberties for the sake of the children will completely ignore crimes against children when it suits them. Can we really trust these organizations to protect children?

The real-time monitoring of messages and outlawing of privacy will not protect children. On the contrary, it would put their communications into the hands of more third parties. The wiser choice would be to encourage parental awareness and conscious use of technology, e.g. not giving children unlimited access to mobile phones or devices and avoiding use of popular social media platforms and messengers.

If these actors truly cared about protecting children, then they would call an end to the genocide & war crimes occurring in Gaza. Instead, the US is rushing to provide aid to Israel in the form of munitions. In the UK, only 80 out of 650 MP’s have called for a ceasefire. Instead, there is more interest in clamping down on and controlling the internet, a crucial resource for all people in a time of great need.

Inter-governmental organizations are pushing towards an internet where our identities are verified and our messages are tracked. With such legislation coming our way all over the world, how can we retain any privacy?

The answer is simple – do not comply. Do not follow along with big tech companies that voluntarily follow legislative guidelines. Find ways to decentralize your use of software. Invest your time into divesting from big tech and learning alternative solutions for communications, storage, and encryption. Given the stakes, there has never been a more important time to divest from these companies and their software.

Thankfully, there are still many ways that individuals can limit their dependence on centralized software services that perform content or AI scanning. We can boycott those Big Tech companies that scan our content including Microsoft, Google, Apple and countless others. It’s just a matter of learning how to take back our technology.

At this point you might be asking:

- How do we continue to find information on the internet without Google’s search engine?
- Or use our computers without Microsoft’s Windows and Apple’s macOS?
- Or use our phones without Google’s Android or Apple’s

iOS?
- Or use our browser without Google’s Chrome, Microsoft’s Edge, or Apple’s Safari? (the oligopoly of these behemoths extends everywhere.)

Solving these problems with alternative software has been the mission of my initiative Take Back Our Tech, and today I am honored to share **5 Ways To Protect Yourself from Incoming Internet Surveillance Bills** with the Unlimited Hangout community.

1. Use a “free” operating system for your computer.

Traditional operating systems (“OSs”) like Windows and macOS are *proprietary* software, which is distinct from *free* software. It’s important to understand the difference between the two, as the topic will come up again. So let’s define proprietary and free software.

Proprietary software, or “non-free software,” is not available for users to study, observe, or change. **As the user, you are given no rights.**

For example, **only the developers** of Microsoft Windows can get a clear look at the code of the operating system and understand what it does. Users have no way to view the code, and verify what the program does.

In contrast, free software (also known as Free & Open Source Software FOSS) gives users rights. The Free Software Foundation, one of the leading organizations behind the Free Software movement, provides an extended definition:

> *“Free software” means software that respects users’ freedom and community. Roughly, it means that* ***the users have the freedom to run, copy, distribute, study, change and improve the software****. Thus, “free software” is a matter of liberty, not price. To understand the concept, you should think of “free” as in “free speech,” not as in “free beer.” We*

> *sometimes call it "libre software," borrowing the French or Spanish word for "free" as in freedom, to show we do not mean the software is gratis.*

You may have paid money to get copies of a free program, or you may have obtained copies at no charge. But regardless of how you got them, you always have the freedom to copy and change the software, even to sell copies.

Alternative operating systems based on GNU/Linux are free software. They offer many intended benefits:

- **Visibility** into changes: Any user or developer can take a look at code updates and ensure that the operating system is not acting unexpectedly or maliciously. For instance, users of the Ubuntu OS fought back against changes that sent search results to Amazon and got the changes overturned.
- **More choices**: Because others can modify and distribute free software at will, far more software choices exist in the free software ecosystem – choices that often outcompete and provide more value than proprietary software.
- **Costs**: All Linux distributions are FREE as in cost. Compare this to paying for Windows activation keys.
- **Freedom**: Your computer will not automatically track every program that you run, as does macOS, or force updates on you, as Windows does (and to which you agree in their terms of service, a document very few take the time to read).

So what are you waiting for? Throw your proprietary software in the trash and enjoy an operating system that respects your freedom and your data.

- If you're still not convinced and want to see all the ways traditional operating systems take advantage of you, read our Leap to Linux article.

- If you're interested in learning how to install a Linux-based OS, please follow #TBOT's guide.
- If you're interested in other Linux learning articles, here is #TBOT's content series on Linux.

Here are some recommendations for free operating systems based on Linux. You can download the .iso file (in which the OS is contained) for each operating system from the following links as well as feature walkthroughs.

Once you've made your decision of OS you can follow the guide linked above to get it installed on your machine.

- (Features) Linux Mint: https://linuxmint.com/
- (Features) KDE Neon: https://neon.kde.org/
- (Features) MX Linux: https://mxlinux.org/

2. Use open-source software on your phone.

The two main choices for traditional mobile operating systems today is Google's Android, and Apple's iOS. These two options make up 99%+ of the global market share of mobile operating systems. With over 6.6 billion phones on earth, the data pipeline to these two companies is incomprehensibly large – they've got real-time data for almost every person on the planet.

Observational studies of both Android and iOS-based phones found that these devices connect back to their parent companies every 5 minutes. In addition, they collect unique device identifiers, phone numbers, locations, and other surprising info.

Although it would be too lengthy to discuss these issues in-depth in this article, if you'd like to see exactly what tracking and data collection occurs on these mobile operating systems, you can read #TBOT's analysis here.

A few alternative operating systems have popped up in recent years that can compete with the likes of Google and Apple.

These operating systems are referred to as “de-googled” operating systems, and are typically built on top of Android’s Open Source Platform (AOSP). This code is maintained by Google, but other developers have been able to build new features on top of it, and more importantly, to remove any behind-the-scenes tracking or data collection.

You can use one of these alternative operating systems today to configure your own “privacy phone.”

I recommend these three operating systems (note that each is compatible with only certain phones):

- GrapheneOS (leading standard for security): https://grapheneos.org/
- DivestOS (device compatibility with 0 Google Services): https://divestos.org/
- LibreMobileOS (a newer OS with great features): https://libremobileos.com/

You can get more information on supported phones and the install instructions on each website.

Alternatively, if you are pressed for time or don’t want to do the research and make the tech decisions yourself, you can get a phone out of the box that comes complete with GrapheneOS and useful free software apps and communication services, through my project Above Phone.

De-googled phones use alternative app stores like F-Droid (where all apps are free software) and Aurora Store (which will allow you to download apps anonymously from the Google Play Store).

Normal Android phones also have access to these apps, but will still suffer from centralized tracking through Google Services. If you have an Android-based phone you can get started with these alternative app stores right away. Get more details on the links below:

F-Droid FOSS App Catalogue: https://f-droid.org/
Aurora Store: https://auroraoss.com/

You may be surprised at how easily you can transition to a de-googled phone – there are user friendly, private, and functional options for almost all of your app needs. You can also use apps like Uber & AirBnb, which don't work without Google services, but there is usually a workaround, like using those services from within a web browser, or by using advanced features like GrapheneOS's sandboxing to isolate Google Services from the rest of your phone.

3. Own your data.

If a major cyber event caused the internet to go down, how would you recover the photos/files/information you stored on cloud services? How would you get the information you needed to prepare for a survival situation?

It would be best to have this information on hand when you need it – not desperately trying to recover it in the event of a cyber disaster.

At a minimum, you should back up all of the following on your local computer instead of on the cloud service you use currently: passwords, legal documents, books, photos, reference material, and maps.

Here are some suggestions to be "cyber-pandemic" ready.

1. Knowledge is power. Download all the books you need in PDF format. A great site to start is PDFDrive
2. Need to navigate offline? Organic Maps (available on F-Droid and for Android phones) lets you download maps of most of the regions on the planet – and you can route to different locations using GPS only (which means you don't need a SIM card in your phone).
3. If you use Google Drive or iCloud, now is the time to export all of your photos, videos, and documents to a

local hard drive. Here's a tutorial on how to export Google Drive files. Here's an tutorial on how to export files on iCloud.

4. Are you managing your passwords in the cloud? Know that cloud password managers are not immune to hacking attempts. The best place for your passwords is in an encrypted password vault on your computer. An attacker would need not only the password vault file on your computer, but also the master password used to encrypt the vault. A collection of software called Keepass offers a cohesive way to manage and sync passwords locally on your computer and on your phone.

4. Support alternatives.

A wide range of software can serve as alternatives in the open-source software ecosystem. I've categorized and listed several great ones below, all of which are programs for Linux computers!

You can also find an important set of core software for Linux with details on how to use it on #TBOT's Open-Source Survival Toolkit. A larger list of programs is available on #TBOT's Open Source Survival Library.

Password Managers

KeepassXC: Offline password manager.
Bitwarden: Cloud-based password manager

Privacy / Security

I2P: Private peer-to-peer networking layer.
VeraCrypt: Open-source cross-platform disk encryption

Browsers

Ungoogled Chromium: A (fork) copy of Google's Chromium engine with tracking removed
LibreWolf: Firefox fork with improved privacy

Falkon: KDE Project's web browser

Email

Evolution: A mail client, calendar, address book, and task manager in one
Thunderbird: Mozilla Foundation's email, chat, and calendaring client
Mailspring: Easy-to-use, modern mail client with integrations to major email providers
KMail: KDE's email client that supports many mail protocols

Communication

Kotatogram: Alternate Telegram client with improved offline features
AnyDesk: Remote desktop / support software
Jitsi: Free video conferencing
Jami: Free and open-source peer-to-peer video conferencing.

Social Media

Nostr: a decentralized social media protocol
PeerTube: Decentralized video broadcasting
Nitter: Alternative twitter front end
Invidious: Alternative YouTube front end
Libreddit: Alternative Reddit front end
Owncast: Self-hosted live video and web chat server

Graphics

Krita: Free and open source digital illustration program
Inkscape: Professional vector-based graphics editor
GIMP: One of the oldest and best- known image editors
Pinta: Bitmap editor similar to Paint.NET
Gravit Designer: Vector-based design app
Blender: End-to-end 3D creation suite

Photography

DarkTable: Virtual light table and darkroom for photography
DigiKam: Personal photo management

Video Editors

Kdenlive: The KDE project's video editor
Davinci Resolve: High-end professional video editor
OpenShot: Easy-to-use, powerful video editor

Video Utilities

OBS Studio: Video recording and live streaming
Kazam: Record videos of your screen
Peek: Record videos and gifs of your screen
Spectacle: KDE's screenshot tool

Technical Tools

Remmina: A remote desktop client
VirtualBox: Create virtual machines

Writing

CherryTree: Hierarchical note-taking application that stores multimedia notes in an encrypted database (not markdown)
Trillium Notes: Build knowledge bases & graphs with this extensible note-taking application (not markdown)
Joplin Notes: Create simple notes and to do lists using markdown

Reading

Foxit PDF: Feature-rich PDF reader.
Sioyek: PDF reader for academic papers.

Office

LibreOffice: Most popular open-source office suite for Linux
OnlyOffice: Collaborative online document editor
CryptPad: Browser-based encrypted document editor
HomeBank: Personal money management

5. Own your communications.

Although social messengers like WhatsApp, Signal, Telegram, and Facebook Messenger can be useful, many of them are not open source. Even the ones that claim to be open source often only make the front end of the application visible for inspection (that part you interact with directly), not the server-side code that is responsible for delivering messages.

Chat protocols like XMPP and Nostr are fully open source, meaning the code is available for the client and server. This is especially important because it means that you can run the server-side software yourself on a computer under your control. This is called *self-hosting,* and it's crucial to censorship resistance and verifying that a software does what it says.

XMPP is over 20 years old and can support tens of thousands of users on a single server. It offers end-to-end encrypted messaging, voice calls, and video calls (as well as files and audio messages). It can be used on computers, phones, and in a web browser, and it's also completely free to join (you can join any public server). It can even be bridged to the phone network (anonymous phone numbers without needing a SIM card anyone?).

It's a wonder why XMPP isn't more well known, but part of the reason could be that it's hard to monetize (make money) on XMPP. The protocol has been used under the hood for major chat services run by big tech companies scaling to millions of users, unfortunately these big companies hid the underlying technology.

Above Phone is attempting to change this. The Above Privacy Suite offers a professional XMPP service with enhanced privacy. It comes in a bundle with 5 other privacy services.

- If you want more information about XMPP, you can read #TBOT's most popular article to date, which gives a comprehensive overview.

- If you want video lessons on how to use XMPP for chats, calls, and video calls, you can check out Above Phone's webinar.

Conclusion

The internet is changing and battle lines are being drawn. On one side, government organizations have become obsessed with invading our personal communications and drastically advancing the ever encroaching surveillance state, supposedly "for the sake of the children." Together with enthusiastic help from Big Tech, they threaten to monitor even single thought, idea, or creation you share on the internet.

On the other side are people who are not going to let that happen. We're the underdogs, a small but growing number of people who are demanding privacy and freedom over convenience. It doesn't have to be their way or the highway when it comes to technology, we can carve our own path, experimenting with software that is friendly and in alignment with our values. Hopefully, this guide can give you a starting point to understand your technology and places to find alternatives.

I encourage you to not only explore and use the software listed in this guide, but to support the developers with financial donations. Their projects may be the key to both surviving and thriving in the growing surveillance state.

Connect with Above Phone project

Connect with Unlimited Hangout

Cover image credit: Franz26