COMPROMISED CONNECTIONS

OVERCOMING PRIVACY CHALLENGES OF THE MOBILE INTERNET

Internews
Local voices. Global change.

Vodafone
Americas
Foundation

A WORLD OF INFORMATION IN YOUR MOBILE PHONE

As mobile phones have transformed from clunky handheld calling devices to nifty touch-screen smartphones loaded with apps and supported by cloud access, the networks these phones rely on have become ubiquitous, ferrying vast amounts of data across invisible spectrums and reaching the most remote corners of the world.

From a technical point-of-view, today's phones are actually more like compact mobile computers. They are packed with digital intelligence and capable of processing many of the tasks previously confined to the realm of desktops and laptops – for example, photo and video editing, conducting financial transactions, and, yes, posting to social network sites!

The mobile carrier industry alliance Groupe Speciale Mobile Association estimates that, globally, there are close to 7.7 billion mobile connections and 4.7 billion unique subscribers, with an annual growth rate of 4.7 percent. According to the independent think tank Pew Research Center's recent global survey, two thirds of the world's population had access to the Internet by the end of 2015 and close to 45% of cell phones were smartphones! As the price of smartphones continues to drop to affordable levels, more people – many who previously had no access to a computer – will suddenly have a world of information in their pockets.

For individuals who use phones as their primary or only Internet-connected device, the growth has been empowering. People living in even remote locations can now accomplish a dizzying variety of tasks, from social networking to making mobile payments, from checking for market alerts to receiving humanitarian information, and from consuming political news to reporting on human rights violations.

Compromised Connections is a brief introduction to emerging security issues facing mobile phones in development. It recommends safety measures that can be quickly adopted – from device safety to data security – and points to resources that may be useful for people interested in following future developments. Ultimately, it advocates a "mobile-first" approach: adoption of an information management strategy that prioritizes the safety of mobile devices and their users.

For civil society organizations around the world, the changes have been no less dramatic. Universal access to devices and Internet connections offers unprecedented opportunity in development and human rights work. It can serve as the fulcrum of civil society organizing, election monitoring, government accountability, budget transparency, critical humanitarian information access during emergencies, and human rights violation documentation. Civil society organizations can have direct and 24/7 access to target communities, and a variety of groups involved in information, advocacy, and rights work can access information, opportunities and choices that they never could before.

Information access through mobile phones, however, works both ways. While we can say with certainty that no other device is helping more people in more places, we also need to acknowledge that with the benefits of increased access and information sharing come a set of risks for the user inherent in the phone, the carrier, and the networks used for data transmission.

The Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and many other international and regional treaties recognize privacy as a fundamental human right. Privacy underpins key values such as freedom of expression, freedom of association, and freedom of speech, and it is one of the most important, nuanced and complex fundamental rights of contemporary age.

For those of us who care deeply about privacy, safety and security, not only for ourselves but also for our development partners and their missions, we need to think of mobile phones as primary computers rather than just calling devices. We need to keep in mind that, as the storage, functionality, and capability of mobiles increase, so do the risks to users.

Can we address these hidden costs to our digital connections? Fortunately, yes! We recommend:

- Adopting device, data, network and application safety measures
- Following the evolving discussion on mobile policy and connectivity
- Instituting a "mobile-first" strategy that focuses on safety and security of users and their devices

RISKS OF USING MOBILE DEVICES

THE PHONE

Mobile phones contain data about contacts, calls, SMS messages, web activity, and even physical location (via GPS and cell towers). Anyone with access to the phone has access to this data, and that may include the developers of popular applications that use this type of information.

THE CARRIER

Cell phone providers have access to a range of customers' data even without physical access to the phone, and may need to share it with other companies. Service providers are subject to laws of the countries in which they operate, and so this information may be shared with regulatory authorities and, by extension, with authorities of other governments with whom intelligence agreements exist.

THE NETWORK

Mobile phones face many of the same security considerations as other internet-connected devices, as well as additional concerns because they use multiple channels when transmitting data, including cell towers, Wi-Fi networks and Bluetooth, each with their own set of privacy challenges.

THE APPS

Applications on phones are rarely built with privacy in mind. Web browsers, instant messaging apps and social networking platforms may expose users' online activity, even when this is not apparent while using the app itself.

INDIVIDUAL SECURITY

The mobile phone has become the primary device for information and communication, letting us carry a lot more of our lives in our pockets. They get constant use. A 2015 study by researchers at Nottingham Trent University found that the average person checks their device 85 times a day and spends up to five hours connected to the Internet (whether through apps or browser). However, this constant synchronization works in both directions. The information on a mobile phone – a log of calls, text messages, browsing history, social network visits, and location – may be available to service providers or other remote parties.

There are physical considerations, as well. **The size and convenience of mobile phones result in relatively easy theft, confiscation, and loss.** Although ten years ago losing a cell phone meant losing contacts stored in the phone and a handful of text messages, today we lose a copy of entire logs of our contemporary digital lives. The stakes are higher now, as the cell phone has become our wallet, our photo album, our social planner, and more.

Adaptation is key in a digitally-connected age. We have already acquired some necessary habits for handling our smartphones, such as learning how to work with a tiny keyboard or remembering to charge the device every day. Starkly missing from these habits, but of utmost necessity, is the need to learn basic safety precautions, too.

A simple but non-exhaustive list of immediately actionable strategies include keeping our phones close to our person at all times, locking them with a passcode, paying attention to what we install, and enabling data wiping functions. Although these measures don't prevent robbery or illegal re-sale of a mobile device, they can protect important personal data and prevent its abuse by others.

In the future, carriers may be more pro-active in helping average consumers protect their devices. The Cellular Telecommunications Industry Association, an international association for the wireless industry, recently introduced its Smartphone Anti-Theft Voluntary Commitment, an initiative formed to discourage reactivation of phones reported as stolen. The hope is that as more countries and more carriers around the world join the initiative, the market for stolen phones will dry up.

However, for now, we have to take responsibility for protecting our phones and their contents.

QUICK TIPS

INDIVIDUAL SECURITY

LOCK THE DEVICE

Several developers are experimenting with new methods of phone protection, including biometrics, but the strongest lock remains a long password instead of a 4- or 6-digit passcode or swipe pattern. The additional complexity (more characters and variety) makes it less likely that anyone will be able to "brute force" an opening into your device.

ENCRYPT IT

A strong password protects your lock screen. Encryption – scrambling photos and files with a mathematical algorithm – improves protection against some other methods of attack. Most smartphones allow you to encrypt your stored data when you enable password-locking.

KEEP TABS ON IT

Both iPhone and Android phones include features that allow you to track the location of your device, lock the screen, change your password or wipe your data remotely (Android users will need to install the Android Device Manager from the Google Play Store first). This protection may not be attractive to all users as it requires enabling location services for the operating system's developer (Apple or Google), but it can be helpful in cases in which a device is lost, stolen or confiscated.

BACK IT UP

Backing up your phone's data can prevent headaches if the device is lost, stolen or confiscated. iPhones and most Android phones (depending on manufacturer) include built-in tools for this. Android users who need a third-party solution may wish to explore free alternatives like Titanium Backup.

NETWORK INSECURITY

Like a kite that depends on the string it's attached to in order to fly, a mobile phone can't work its magic unless it's tethered to something stable – a cell tower. That connection is constant. A mobile phone sends out pulses, or "pings," to identify itself and let cell towers know it's in the area. It then continues to send out pings to keep tabs on new potential connections as it moves around. Without this conversation taking place in the background, even when we are not using the device, we couldn't send and receive instant messages or receive phone calls. And that broadcast, necessary as it is, raises some possible concerns.

One possible concern is **location tracking**. As a signal passes through a network of cell towers, it can expose a user's location. Someone interested in locating a phone (and through it, the user) can compare the signal strength of a phone on multiple cell towers, triangulate the information, and pinpoint the phone's approximate location. While this data may not be accessible to petty criminals, mobile network operators can be legally required by law enforcement to reveal that information. The TED talk called "Your Phone Company Is Watching," in which German MP Malte Spitz reveals how data was collected on his own whereabouts over a six month period, is an example of this in the real world. In some cases, authorities are very open about this sort of data collection: in 2011, China planned to capture location data of all phone users in real-time, ostensibly to alleviate traffic congestion, though it may have had other uses.

Another concern is **network authentication**, following reports of law enforcement and intelligence agencies using Stingray devices (or "IMSI catchers") to monitor calls and callers. Stingray devices impersonate cell phone towers and send out signals that trick phones into revealing identifying information about the phone and, by extension, the phone's owner. They also, with proper configuration, can force cell phones to communicate without encryption. The increasing use of Stingray devices raises significant privacy concerns, according to the American Civil Liberties Union.

Of course, cell networks aren't the only type of network that mobile phones use these days. When the phone's Wi-Fi is turned on, for instance, the phone sends out signals that include its MAC (Media Access Control) address, a unique identifier that's hardcoded into the device. Although due to limited range Wi-Fi itself is not very useful for surveillance, **MAC addresses can be tracked across Wi-Fi hotspots** revealing information about when a user enters or leaves a specific place, and what they were doing online in these places.

Public Wi-Fi networks have also been used for "man-in-the-middle attacks." These are attacks in which Wi-Fi access points are designed to look legitimate (e.g. "Free Wi-Fi"), but are actually operated by an attacker. Users who connect to these fake Wi-Fi networks can be eavesdropped on or directed to fake websites to obtain sensitive passwords and other information.

While privacy concerns related to Stingray and public Wi-Fi are real, spyware is becoming the most common method for tracking phone users. **Off-the-shelf mobile spyware products** enable interception of emails, text messages, and calls, and in some cases spyware can remotely access smartphone microphone or camera. According to Flashware Spyware Report, published in 2014, even many flashlight apps in the Google Play Store asked for permissions enabling them to track GPS coordinates, access text message history, and scan call logs.

Clearly, network insecurity poses a special challenge in the modern digital landscape. The same infrastructure that empowers us to stay connected with friends and colleagues in the field also, in order to work, must track information that is unique to us and our devices, opening us to a level of scrutiny on a scale that we haven't experienced previously.

QUICK TIPS

NETWORK INSECURITY

USE APPS WITH ADVANCED PRIVACY

While not allowed in all countries, specialized applications are available for iPhone and Android phones that allow them to protect the content of their instant messages and online phone calls (also called VOIP). One example is Signal Private Messenger from Open Whisper Systems. It allows users to authenticate one another's identity, after which they have the option to protect their chats and online calls by default.

SECURE YOUR CONNECTION

Public Wi-Fi access points and data connections to your phone company may not be secure by default, potentially exposing information about you and your online habits such as web browsing, email and instant messaging. A VPN (Virtual Private Network) can improve privacy by establishing a protected connection between your phone and a server at another location before then connecting to the service you wish to use. Free solutions are available: Psiphon 3 is free for Android users, while iPhone users may wish to investigate HotSpot Shield free edition.

TURN OFF WI-FI

That goes for Bluetooth, too. If you aren't actively using those types of connections, consider turning them off to reduce your footprint (and save on battery life between charges).

TREAT THE PHONE APPROPRIATELY

If you or colleagues work in environments in which privacy is not an option, tailor your calls with that in mind. For instance, reserve sensitive conferences that may involve financial information and the like to in-person meetings.

MALWARE ATTACKS

Malware attacks against mobile phones have increased exponentially in the last half-decade, and indications are that these types of attacks are here to stay. Pulse Secure, a private firm that focuses on connectivity for businesses, reports in its 2015 Mobile Threat Report that it identified nearly one million (931,620) unique malicious applications that year alone.

Malicious software or Malware is any app that attacks a user's phone in order to carry out detrimental acts without the user's consent. Recent examples include tollware (apps that force the user's phone to send premium SMS messages or make premium rate calls in order to charge the device's real owner), ransomware (apps that hold a device hostage by encrypting it and demanding payment to decrypt and release it), and spyware (apps that gather user data including contact lists, phone logs, text messages, location, and browser history, without obtaining the user's express consent). These apps may ask for unusual permissions when installing, and connect the phone to a command-and-control server.

Where does malware come from? Typically, malware is spread when a user downloads an application outside official app stores like Apple's App Store, the Google Play Store, or the Windows Phone Store. While Apple and Google have processes in place to vet the apps they distribute online, many users, particularly in the Middle East and Asia, use unregulated third-party app stores when seeking software, according to the Mobile Threat Report.

International Data Corporation, a market intelligence firm in the information technology sector, reports that Android phones dominate the mobile phone market, with an 83% marketshare in 2015. It is perhaps not surprising then that **the largest percentage of malware out there (some 97%) targets Android phones**.

Another common way that phone owners pick up infections is through **sideloading**, a term that refers to the transfer of data between two devices, in this case between a computer and a mobile device such as a smartphone.

A majority of devices come pre-configured to use an official app store, and the ability to sideload apps is usually disabled by default – a useful security feature, since installing software from unknown sources carries more risk. But the filter can easily be disabled manually.

There are many reasons that people decide to sideload apps that don't come from official online stores. Some do it to avoid slow download speeds and high data costs or to try out pirated versions of applications that would normally cost a lot of money. Localization is also a draw: let's say we want the latest version of Twitter on our device, but it isn't yet available in the area we live or in our language. A quick search online or a visit to our local phone market leads us to someone offering a version customized for us. We trust Twitter, so what could go wrong? Well, that downloaded file could have malicious code weaved in, dormant until it is installed on your device. Most users don't stop to consider that apps distributed through unofficial sources could have been tampered with.

QUICK TIPS

MALWARE ATTACKS

UPDATE OPERATING SYSTEMS AND APPS

Updates can protect iPhones and Android phones against vulnerabilities that are discovered, and quickly exploited, by hackers. Users should regularly visit the official app store for their platform to get these updates.

AVOID "SIDELOADING"

While it is a convenient and often economical method for installing popular applications, sideloading is also a common source of malware infection.

INSTALL AN ANTIVIRUS

Many of the software companies that make antivirus applications for PCs also make similar apps for mobile devices. These apps frequently try to up-sell you with advanced features, but offer basic protection for free. One example is Avast! Mobile Security, which is ranked among the most effective by analysis firm AV-Test.org in January 2016. It's available on the Google Play store.

LIMIT APP PERMISSIONS

Both iPhone and Android phones let users control (to varying degrees) the access that apps have to information on the device and to networks that the phones uses. See the Further Resources section of this guide for information on how to do this yourself.

MAKE IT A POLICY!

Consider adding these steps to a larger security plan for your organization and those of partners.

LOOKING AHEAD

As ICT-aided information flow becomes a necessary feature of modern life, many more people will be connecting to the Internet globally, and with much higher frequency. As mobile phones lead the charge for us and our collaborators as our primary Internet-connected devices and thus gateways to many of our tasks, we need to rethink how we view ICT security.

The growing and rapidly changing interaction between ICT and society will continue to push a wide range of human rights concerns to the forefront. In response, we need to carefully think about how we harness the power of these technologies, while continuing to protect and advance freedom of expression and privacy online.

In addition to practicing better device hygiene at the individual level by keeping operating systems and apps up to date, only installing apps from developers we trust, controlling permissions, etc., we also need to focus on network security. As we leverage the mobile platform, creating newer and more innovative apps, the platform itself will continue to create new security challenges for organizations. These challenges will continue to evolve as technology continues to advance.

Just as mobile technology brings great benefits, its risks are undeniable. A 2015 study by IBM Security and the Ponemon Institute found that just in the year 2014, one billion personal data records were compromised by cyber-attacks, and that at any given time, mobile malware is affecting 11.6 million mobile devices. The study also found that nearly 40 percent of large companies, including many of the Fortune 500s, were not taking precautions to secure their mobile apps against vulnerabilities.

When apps have not been tested for extreme conditions, it puts not just the device and the app, but also individuals, organizations, and the issue itself at risk. Human rights organizations and other advocates will need to integrate research and truth-testing of applications into their workplans in order to responsibly safeguard the transmission and the storage of data they and partners collect.

In short, we need to evolve in line with the increasing threats that are emerging in the security landscape. We need to go for solutions that can offer a holistic approach towards fighting these threats. It is time for organizations that use mobile in their work to adopt a comprehensive mobile security strategy. The rights community can learn from the humanitarian community that works with ICT in extreme (extremely risky) conditions.

FURTHER RESOURCES

There are many online resources available to help users make informed decisions about using mobiles wisely. While mobile security and digital privacy are fast-evolving topics (with new issues, threats and protections emerging each day), the websites below, compiled in March 2016, and loosely grouped by topic, offer guidance, research and tools to get started.

INDIVIDUAL SECURITY

SUMMARY OF THE ISSUES

The Internews Innovation blog summarizes mobile security threats and solutions, and a more recent post from the Electronic Frontier Foundation tackles the same topic in its Surveillance Self-Defense guide.

HELP WITH CREATING STRONG PASSWORDS

Free applications like KeePassX help you generate strong passwords using parameters that you set, and a guide by Security-in-a-box explains what makes some passwords stronger than others.

REPORT: WHAT COULD BE EXTRACTED FROM AN IPHONE IN 2013?

According to documents obtained by the American Civil Liberties Union that year, quite a lot. Experiences like this one may explain why Apple has adopted a 10-attempt limit on iPhones to prevent brute-force unlocking.

STEP-BY-STEP SETUP FOR ANDROID

Security-in-a-box provides a step-by-step secure setup guide for Android users including setting up encryption and other security-related settings on the device.

TEACHING OTHERS ABOUT THESE CONCERNS

The SaferJourno project at Internews and the multi-organizational program LevelUp offer free lesson plans and other training resources to organizations looking to spread knowledge about mobile security, among other topics.

TOOL: REMOTE WIPING

Lookout Mobile Security is one of several third-party applications that provide remote wiping and location services for older Android phones and iPhones that may not support those newer features natively.

NETWORK INSECURITY

CITIZEN LAB: "THE MANY IDENTIFIERS IN OUR POCKETS"

This summary report from University of Toronto quickly explains exactly what identifying information can be tracked, on which networks and by whom.

RESPONSIBLE DATA FORUM: "CODE OF CONDUCT FOR CROWDSOURCING"

This fascinating work in progress attempts to provide, "a list of things that any organization that launches a digital crowdsourcing project must and should do," written by the people who run such projects. The list includes communicating certain network security and surveillance concerns to colleagues and partner organizations, and implies a roadmap for any organization that plans to conduct crowdsourcing projects in sensitive environments.

RESPONSIBLE DATA FORUM: "MOBILE PRIVACY AND INFORMATION SECURITY IN GLOBAL DEVELOPMENT PROJECTS"

This paper from the New America Foundation defines five principles it recommends for organizations designing development projects, including steps that should be taken to protect data from third party surveillance.

SECURITY-IN-A-BOX: "USE MOBILE PHONES AS SECURELY AS POSSIBLE" AND "USE SMARTPHONES AS SECURELY AS POSSIBLE"

These modules, intended for end-users, include practical tips for using phones on insecure networks, tutorials for configuring the phone, as well as many recommendations for applications that can help.

SURVEILLANCE SELF-DEFENSE: "THE PROBLEM WITH MOBILE PHONES"

This overview of mobile phone insecurity, from the Electronic Frontier Foundation, includes clear summaries related to how cell phones work and why they are inherently insecure.

MALWARE ATTACKS

ANDROID PERMISSIONS: "ANDROID PERMISSIONS EXPLAINED"

This resource, posted on AndroidForums, provides a step-by-step walkthrough for the Permissions feature.

AN EXAMPLE OF SPYWARE USE

University of Toronto's Citizen Lab analyzes uses of spyware called FinFisher and what it exposes on different mobile platforms (e.g. iOS, Android, Blackberry) in an article called "The SmartPhone Who Loved Me."

IOS PERMISSIONS: "ABOUT PRIVACY AND LOCATION SERVICES"

This official support resource for iPhones includes details about restricting permissions for applications on iPhones.

A MALWARE CASE STUDY: TIBET

University of Toronto's Citizen Lab details its findings regarding the use of malware that was apparently crafted to target Tibetan activists in "Permission to Spy: An Analysis of Android Malware Targeting Tibetans."

MOBILE ANTIVIRUS APP COMPARISONS

Analysis firm AV-test.org posted a performance chart ranking more than 25 AV applications.

THE POTENTIAL SCOPE OF ONE MALWARE ATTACK

"950 Million Android Phones Can Be Hijacked" from July 2015 announces the "Stagefright" vulnerability – which has since been fixed in recent releases. The scope of the event underlines the importance of keeping applications and the operating system of a phone up-to-date.

A SUSPICIOUS (AND POPULAR) APP CASE STUDY IN CHINA

"Baidu's and Don'ts" is a report, also from the Citizen Lab at University of Toronto, that explains recent concerns about the behavior of the Baidu Browser, used primarily in China on Android.

MORE RESOURCES

ACLU'S FREE FUTURE BLOG

The ACLU's Free Future blog advocates for an uncensored Internet, and for it to be given as much First Amendment protection as traditional media such as books, newspapers and magazines.

ARS TECHNICA: RISK ASSESSMENT

The Risk Assessment section of ArsTechnica.com includes daily stories related to digital security and "hacktivism", such as malware attacks affecting popular phone models.

ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

The Association for Progressive Communication organizes seminars and provides practical information related to basic privacy practices in the digital age. The website's Publications section includes security toolkits designed for human rights defenders.

ATOMIZED SECURITY PLAN FOR ORGANIZATIONS

This library of security recommendations, broken up by topic (e.g. "email", "passwords", etc.) was created by advocacy research group Engine Room and added to by members of several organizations.

THE BERKMAN CENTER FOR INTERNET & SOCIETY

The Berkman Center for Internet & Society regularly tackles difficult legal and technical questions surrounding digital privacy and freedom of expression.

A BRIEFING ON INFORMATION SECURITY FOR HUMANITARIAN NGOS

This report, from the European Interagency Security Forum and based on interviews with security and information managers of humanitarian NGOs, makes risk management a part of the information management process. Page 6 contains a useful flow-chart for assessing what information needs to be solicited and stored.

CENTER FOR DIGITAL DEMOCRACY BLOG

The official blog of Center for Digital Democracy a leading US-based consumer protection and privacy group, follows a range of issues including legal challenges for organization that store data.

CITIZEN LAB

The Citizen Lab, part of the Munk School of Global Affairs as the University of Toronto, conducts original research on digital surveillance, censorship and human rights, and provides digital freedom profiles for more than 60 countries.

FREEDOM HOUSE

Freedom House maintains, among other useful resources, an annual assessment of Freedom on the Net, which grades countries around the world based on local policy.

GLOBAL DIGITAL DOWNLOAD

The Global Digital Download from Internews delivers daily and weekly summaries of technology developments from around the world related to privacy, censorship and freedom of expression.

GLOBAL NETWORK INITIATIVE

The Global Network Initiative, a non-profit devoted to promoting privacy and freedom of expression, makes its reports and panel discussions on topics such as "Encryption and Human Rights Online" available for free.

LIBERATION TECHNOLOGY

The Liberation Technology project at Stanford University conducts seminars, original research and practical labs for people interested in the challenges of advancing human rights through technology and data.

PROTECTING HUMAN RIGHTS IN THE DIGITAL AGE

This thorough overview of all components of Internet security, researched and written by the Global Network Initiative, can help organizations understand which components apply to their work in the field.

RIGHTSCON

RightsCon, an annual gathering of technologists, human rights workers and privacy advocates from around the world, includes presentations and training events over several days. The Past Events section of the website features video clips on a variety of topics, including "Real World Threats for Human Rights."

SAFERJOURNO

This free, downloadable guide from Internews identifies and explains common threats to digital privacy, and provides recommendations for solutions.

SECURITY IN-A-BOX

This venerable online resource explains many of the most common risks that human rights workers and other advocates face in the digital age and suggests creative solutions with detailed tutorials and walkthroughs.

WORLD WIDE WEB CONSORTIUM (W3C)

The World Wide Web Consortium is an international community that works to develop web privacy standards.

WIRED: THREAT LEVEL

This security-oriented section of Wired covers privacy technology in current affairs in a accessible language.

ACKNOWLEDGEMENTS

Written by Manisha Aryal & Dylan Jones
Icons by Roberto Colombo and Designify.me from the Noun Project
Cover image by Moreno Berti and used with a CC BY-ND 2.0 license
Page 4 and 10 images by Pabak Sarkar and used with a CC BY 2.0 license
Design and layout by Nikki Bourassa

Internews
Local voices. Global change.

Vodafone
Americas
Foundation