GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Digital surveillance

Elijah Sparrow
LEAP Encryption Access Project
https://leap.se

This report examines the properties that make digital communication prone to surveillance and provides a general overview of where and how this surveillance takes place. For our purpose here, any internet or phone-based communication is considered to be digital communication, but we exclude from consideration other forms of surveillance such as direct observation or photography.

The properties of digital communication

It is no easy task to pinpoint what we mean when we say "surveillance". As a first approximation, David Lyon defines surveillance as "the focused, systematic, and routine attention to personal details for purposes of influence, management, protection, or direction." This definition tries to convey the way in which surveillance has historically functioned as a necessary aspect of maintaining modern society,[1] for example, in sorting citizens from non-citizens, the sick from the healthy, the credit worthy from the credit risks. He then immediately goes on to note that surveillance is often not focused, systematic or routine at all – for example, in the case of dragnet surveillance that captures information from the digital communication of everyone without any evidence of its efficacy. What are we to make of surveillance in a digital age, where the capture and processing of personal information by powerful actors is not just routine but ubiquitous? Increasingly, surveillance does not seem an activity undertaken for simple "influence, management, protection or direction", but instead seems to be much more, constituting the core security strategy of many nation-states and the core business model for the largest internet firms, credit card companies, and advertisers.

Most historians of surveillance likely agree with Lyon's assertion that "digital devices only increase the capacities of surveillance or, sometimes, help to foster particular kinds of surveillance or help to alter its character."[2] It is worthwhile, however, to ask what precisely is different about "digital", and how this transformation of surveillance scale and character might represent something substantially new.

Perfect digital copy

A good analogy for the key difference between analogue and digital communication is to compare speech with the printed word. Without modern audio equipment, it is difficult for a human to reproduce speech exactly, but it is very easy to reproduce written words. Like written words, digital information is encoded into discrete and reproducible components. Because of this, digital information is always copied perfectly, unlike analogue communication, where data was conveyed via imprecise and ephemeral voltage or frequency levels. More to the point, digital information can only be copied. You cannot move digital information from one place to another without making a perfect copy. The copy operation frequently fails, but the process is always audited for errors and repeated until the copy is perfected.

Many points of capture

When communication is digital, surveillance lies at its very heart. Because every possible step in the transmission and reception of digital communication results in a perfect copy, the information at every step is exposed for easy capture. As we transition to all communication being digital, we move into a world with an explosion in the potential sites of surveillance capture. At the same time, the relatively centralised nature of the core backbone of the internet makes it possible to monitor most of the world's traffic from a few key locations.[3] Also, the

1 Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press, p. 14.

2 Ibid., p. 15.

3 Although most people think of the internet as decentralised, it is more accurate to describe the topology as polycentric. The backbone core of the internet that carries nearly all the traffic is owned by a handful of "Tier 1" carriers, making it possible to capture most of all internet traffic by listening at the points of exchange between these carriers. This is less true of traffic from the large internet sites, such as Google, Facebook and Netflix, as they have recently installed content delivery networks "inside" the networks of the large internet service providers.

rapidly falling cost of sensors to convert real-world inputs into digital signals has resulted in a proliferation of these sensors in our environment, from our consumer devices to agriculture to sensor networks designed to improve urban life.

Data immortality

Although your personal device might fail, information stored on servers in digital formats effectively lives forever. Physical storage mediums often have short life spans, but information is nearly always stored in duplicate, so that when one physical device begins to fail the information is automatically mirrored to another storage device. Error-correcting protocols ensure that this endless copying never results in an imperfect copy. As the amount of storage available per dollar continues to grow exponentially, there is often no need to ever throw anything away, even for very large datasets.

Automation

The capture, storage and analysis of digital information is largely automated, unbound by the limitations of available human labour. The former East German secret police employed as many as two million informants,[4] but today it would require only a handful of off-the-shelf network monitoring devices, placed in key locations, to far surpass the Stasi's reach. The result of this automation is that both state intelligence services and internet businesses that monetise user information have taken the general approach of capturing everything, when practical, with the idea that the data might be useful in the future.

To be sure, there are limits to how much information can be captured and effectively analysed. These limits, however, have been pushed back faster and farther than most observers expected, as both nation-states and private firms have invested heavily in ways to store and process more data.

High confidentiality

In the past, when surveillance was labour intensive and available only at a few specific sites in the communication process, it was possible to establish a legal framework that adequately sanctioned and controlled the when, where, who and why of state surveillance. Digital communication has destroyed this in two ways: first, the barriers to entry for capturing information for surveillance are very low; and second, the only way to prevent nearly everyone from doing so is to encrypt the data, but this also prevents state-sanctioned surveillance. Data is either widely vulnerable to surveillance by a variety of actors, many nefarious, or it is secure, encrypted, and eludes state control. In practice, of course, this is still not entirely the case, because most security products are deeply flawed and determined state actors and criminal organisations are able to bypass these systems. The poor quality of existing security products is changing rapidly, however, as more people become aware of the level of surveillance in their lives and seek out increased security.

One potential middle ground that could allow sanctioned surveillance but prevent unsanctioned compromise is the so-called "key escrow" technology, such as the type promoted by the United States (US) government in the 1990s under the Clipper Chip programme. In practice, this technology has not proven itself to be secure, and widespread adoption would require making normal cryptography illegal, a move only likely in the most repressive contexts.

So far, the mathematics behind common encryption standards, such as OpenPGP or AES, have generally held strong and those seeking to decrypt confidential communication are fighting an uphill battle. Typically, attacks against encrypted communication exploit other weaknesses, but are unable to break the encryption itself.[5]

Low anonymity

If communication can theoretically be made highly confidential without much effort, the opposite is true of anonymity. It is possible, for example, to identify a unique fingerprint of the radio signals produced by all wireless digital devices. In general, every electronic device emits electromagnetic radiation that can be used to identify it and often to eavesdrop remotely.[6] Even our web browsers advertise to every web server a set of attributes that can comprise a unique fingerprint.[7]

Government and private sector organisations often argue that the certain datasets they collect and maintain are anonymous because they do not include the real names of people. In reality, re-

4 Koehler, J. (2000). *Stasi: The untold story of the East German secret police*. Boulder: Westview Press.

5 One of the top cryptographers in the world, Adi Shamir, has said "cryptography is bypassed, not penetrated." This is not to imply that systems are generally secure. Far from it – they are usually entirely insecure, but rarely because of a fundamental flaw in the cryptography. Peter Gutmann's excellent presentation "Crypto Won't Save You Either" covers most of the major security problems in recent memory and details how attackers simply bypassed encryption: www.cs.auckland.ac.nz/~pgut001/pubs/crypto_wont_help.pdf

6 Elliot, M. (2013). Noise Floor: Exploring the World of Unintentional Radio Emissions. Presentation at DEF CON 21. Video: www.youtube.com/watch?v=5N1C3WB8c00, slides: https://docs.google.com/presentation/d/1Z_IRt6R2FL7POeY4j-pYGLDAIAdEHprQY13f-NVIfwE

7 Eckersley, P. (2010). *How Unique Is Your Web Browser?* https://panopticlick.eff.org/browser-uniqueness.pdf

searchers have been able to de-anonymise nearly every such dataset when given an opportunity.[8] For certain types of information, like location and relationships, it often requires only a few points of data to unmask a person's identity by correlating with another dataset in which real names are known.

The rise of packet-switched networks, like the internet, has also made anonymity difficult. The historical transition from analogue to digital was accompanied by a similar transition in networking from circuit switching to packet switching. Where once a single continuous circuit was required to make a phone call, now a phone call is digitised and converted into millions of tiny packets, routed through equipment that handles millions of other calls. Every packet contains a source and destination headers so that each device in the network knows where to forward the packet on to. Packet-based routing has revolutionised communication as much as digitisation has by allowing the massive investment in old copper cables to be re-purposed for digital networks that can transport millions of times more data. One consequence of packet-switched networks is that it is extremely easy, at many points and times in the network, to determine the flow of who is communicating with whom.

All digital data carried over a network is converted into packets, with different communication protocols layered on top, such as phone calls, email and financial exchanges. These higher-level communications involve their own, and distinct, information regarding the from, to and when of the relationship, but the general idea is the same. This type of transactional or relationship data, recently dubbed "metadata" in the press, is structured and efficient to store, lending itself to various types of powerful analysis that can reveal surprising information from seemingly innocuous data.

Attempts to mask these associations with tricks such as onion routing and data mixing are mostly experimental, make communication much slower, and are rarely used.[9] Because the success of these anonymising networks is dependent on their scale, anyone seeking anonymity in their digital communication is fighting an uphill battle until such approaches become commonplace.

In brief, surveillance of digital communication is ubiquitous, automatic, and effectively lives forever. In the future, people will likely find it easy to encrypt the content of their communication, but their pattern of communication and relationships will likely be difficult to keep from being exposed.

A brief taxonomy of digital communication surveillance

In examining where surveillance of digital communication takes place, we divide surveillance into two categories: attack or capture.

Points of attack

Attacks are attempts to subvert the way a computing system is supposed to work. Attacks might be legal and ordered by a court, carried out by a government without legal authorisation, or entirely extralegal. Attacks might be carried out by private contractors, government agents, or organised crime. Regardless of who is carrying out the attack, and for what purpose, attacks share many common characteristics.

Network interposition: In a man-in-the-middle (MiTM) attack, the attacker interposes themselves in the communication stream between two parties in order to modify the data. Modified traffic can be used to steal authentication information, modify web applications, or inject Trojans into the target's device. Although network interposition attacks are typically associated with powerful surveillance agencies like the US National Security Agency (NSA) and Government Communications Headquarters (GCHQ) in the United Kingdom (UK), even small governments with very limited resources have made effective use of MiTM attacks against dissidents (for example, the Tunisian government in the lead-up to the Jasmine Revolution of 2011).[10] Regardless of the physical location of the target, a MiTM attack can be launched from nearly anywhere, even on a modest budget, due to critical vulnerabilities in the protocol that negotiates routes on the internet.[11] Mobile devices are also vulnerable to MiTM attacks

8 One of the first examples of surprising de-anonymisation concerned the "anonymised" dataset released by Netflix for a competition to improve their recommendation engine. Narayanan, A., & Shmatikov V. (2008). *Robust De-anonymization of Large Sparse Datasets*. www.cs.utexas.edu/~shmat/shmat_oako8netflix.pdf

9 Onion routing is a process where a communication stream is routed through many computers, each one unaware of all the others except for their immediate peers. It is used in low-latency anonymisation networks like Tor. Data mixing is a process where many asynchronous packets of data or messages are combined into a common flow, and then potential routed through multiple mixing nodes. Data mixing is used in high-latency anonymisation networks like Mixmaster. Both processes attempt to anonymise communication by using many servers, but each approach makes different trade-offs.

10 O'Brien, D. (2011, January 5). Tunisia invades, censors Facebook, other accounts. *Committee to Protect Journalists*. https://cpj.org/blog/2011/01/tunisia-invades-censors-facebook-other-accounts.php

11 Pilosov, A., & Kapela, T. (2008). Stealing The Internet: An Internet-Scale Man in the Middle Attack. Paper presented at DEF CON 16. https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

from cheap "IMSI catchers", widely used by law enforcement.[12]

Physical compromise: The large intelligence agencies have top-secret product catalogues of hundreds of high-tech equipment that can be hidden inside a device or modify a device to allow eavesdropping,[13] sometimes installed in new equipment before it reaches the customer.[14] But an attacker seeking to physically compromise a device does not need the budget of the NSA: for a few dollars, anyone can order online a tiny USB dongle that snaps between a keyboard and a computer and allows the attacker to record every key stroke.[15] Because physical compromise is very difficult to detect, computing devices that have been physically in the possession of an attacker should not be trusted.

Remote exploit: Software, in general, is full of unknown security vulnerabilities waiting to be discovered. Most of the time, these vulnerabilities are identified by responsible researchers who notify the software authors so that a fix can be made available or an update automatically applied. Attackers are able to take advantage of the gap in time between when a vulnerability is fixed and when this fix is actually applied in order to exploit the flaw and hijack a computer or steal information. If a vulnerability is first discovered by an attacker it is called a "o-day", because there have been zero days since the vulnerability has been known to the public or the software developers. Various governments, as well as some criminal organisations, spend large amounts of money developing o-days and purchasing them on the black market.[16]

Social engineering: Attackers often rely on fooling humans rather than computer systems, a process called "social engineering". Humans can be remarkably easy to trick. For example, when researchers scattered random USB memory sticks in a parking lot, most of the people who found them plugged them into their organisation's private network,[17] an extremely insecure practice that can result in a MiTM attack or provide an easy entry for a Trojan.[18] One highly effective and low-cost form of social engineering is called "spear phishing", where the attacker uses some bit of personal information about the target to trick the target into opening a hostile Trojan. Many people, for example, would open an email attachment that appears to come from a friend or colleague. Social engineering can also be as simple as impersonating someone on the phone.

Software updates: In some cases, the software update system designed to apply security fixes to a device can itself be the delivery pathway for a Trojan or other malicious code. Sadly, few update systems are very secure.[19] The United Arab Emirates, for example, used the BlackBerry update mechanism in order to install remote surveillance capabilities on all BlackBerry customers in the country (without the knowledge of or approval from BlackBerry).[20]

Third-party compromise: With the recent rise of cloud computing, nearly all users rely on third parties to keep some or all of their sensitive information safe. As consolidation has resulted in fewer third parties holding an ever larger cache of personal data, attackers and governments have turned their attention to these third parties as an efficient, centralised source of surveillance data.[21] The daily parade of data-breach headlines is evidence of the grossly inadequate security practices by many of these third parties.

Trojans: A Trojan is a type of computer virus disguised as a benign programme, or it may even be hidden inside a modified version of a common application. In a "phishing" attack, the target installs

12 Stein, J. (2014, June 22). New Eavesdropping Equipment Sucks All Data Off Your Phone. *Newsweek*. www.newsweek.com/your-phone-just-got-sucked-255790

13 Appelbaum, J., Horchert, J., & Stöcker, C. (2013, December 29). Shopping for Spy Gear: Catalog Advertises NSA Toolbox. *Der Spiegel International*. www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

14 Greenwald, G. (2014, May 12). How the NSA tampers with US-made internet routers. *The Guardian*. www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden

15 As of this writing, there are dozens of key loggers available on Amazon.com, most for less than USD 100 and many with remote wireless access.

16 Menn, J. (2013, May 10). Special Report - U.S. cyberwar strategy stokes fear of blocback. *Reuters*. in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510

17 The fault here is not really human error, but human error only in the context of very poorly designed operating system security. Edwards, C., et al. (2011, June 27). Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy. *Bloomberg News*. www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html

18 Greenberg, A. (2014, July 31). Why the Security of USB Is Fundamentally Broken. *Wired*. www.wired.com/2014/07/usb-security

19 Cappos, J., et al. (2008). *A Look in the Mirror: Attacks on Package Managers*. https://isis.poly.edu/~jcappos/papers/cappos_mirror_ccs_08.pdf

20 Coker, M., & Weinberg S. (2009, July 23). RIM Warns Update Has Spyware. *Wall Street Journal*. online.wsj.com/news/articles/SB124827172417172239

21 Gellman, B., & Poitras L. (2013, June 6). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *Washington Post*. www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

the Trojan themselves, fooled into believing the application is legitimate. When used by governments, the Trojan is often installed manually when the device is out of the possession of its owner or via man-in-the-middle network attacks. Although many Trojans are created by those sending "spam" or organised crime, Trojans are also big business: one Trojan developed by Hacking Team, an Italian surveillance company, is used by over 60 governments and allows the operator access to nearly all aspects of a target's mobile device.[22]

Usability error: At present, most software that allows you to communicate securely is highly sensitive to mis-configuration or misuse, providing many opportunities for attack. Many chat applications, for example, have a default setting that will allow an attacker to bypass secure connections between the client and the server.[23] In 2008, the default setting in Thunderbird caused thousands of German users to silently drop transport encryption when their internet service provider (ISP) accidentally disrupted the secure connection negotiation (since fixed).[24] The very concepts required for confidential communication, such as public and private key or key fingerprints, are deeply confusing for many users.[25]

Points of capture

Rather than an attack that exploits a flaw, some forms of surveillance are an incidental or core function of the system itself.

Devices: Nearly every end-user computing device that facilitates digital communication retains a wealth of personal information as part of its normal operation. Particularly in the case of mobile devices, this information likely includes web browsing history, location history, call records, photographs, and a record of messages sent and received. User devices also often store a copy of authentication credentials that can be used to gain access to information stored by third parties. Some devices are very small or even invisible: for example, an "embedded system" containing a rudimentary computing logic and memory capacity can be found in USB memory sticks, some RFID chips,[26] and appliances. Despite their simplicity, these embedded systems can be programmed to record information about the user, as in the case of the 2006 World Cup where the event tickets themselves contained an RFID chip that both reported personal information to authorities whenever the ticket passed a scanner and also recorded on the ticket itself a history of locations the ticket had been.[27]

Device emissions: As noted previously, every device, and many applications, emit unique signatures that can be used to track the location, behaviour or internal workings of a device. These unique signatures take many forms: by design, web browsers present uniquely identifying information to every website they visit; by design, every mobile phone has a unique and unchangeable tracking identifier that is logged by cell phone towers; by accident, devices emit unique electromagnetic radiation that can remotely reveal the screen contents; by accident, central processing units (CPUs) emit low level noise that a remote listener can use to extract private keys;[28] and so on. What counts as a device will soon become difficult to define, as consumer goods such as clothing, watches, appliances and tickets start to include tiny embedded systems – even food[29] may soon be tracked via RFID.

Networks: Surveillance can take place at every step in a data packet's journey from source to destination. Networks may be monitored close to an endpoint, as when an IMSI catcher is used to monitor the traffic of a target mobile device, at the ISP level, or at the level of the internet backbone where most traffic eventually flows. Because the internet is polycentric, relying on a handful of large carriers for connections among ISPs, a small number of strategic listening posts are able to monitor a high percentage of all traffic. Typically, large intelligence agencies monitor traffic near the backbone, small governments will monitor all the traffic in and out of their country (typically at the ISP level), and everyone takes part in monitoring close to the endpoint (including organised crime). The US and UK use network surveillance to build very large databases of

22 Zetter, K. (2014, June 24). Researchers Find and Decode the Spy Tools Governments Use to Hijack Phones. *Wired*. www.wired.com/2014/06/remote-control-system-phone-surveillance

23 By specification, chat applications that support the XMPP chat standard must use StartTLS for secure connections, but StartTLS will downgrade to plain text and insecure connections if the TLS negotiation fails (which is not hard for an attacker to cause). Only if the chat application is configured to notify the user of this downgrade, or prevent it, will the user be assured of a secure connection. This same vulnerability exists in many email clients.

24 Heise Security. (2008). Eingriff in E-Mail-Verschlüsselung durch Mobilfunknetz von O2. heise.de/-206233

25 Whitten, A., & Tygar J.D. (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. www.gaudior.net/alma/johnny.pdf

26 RFID (radio frequency identification) is a technology that allows an item to report a globally unique identifier when the tiny RFID chip is passed near a scanner. Some RFID chips, however, also contain embedded systems with a small degree of computing logic and memory capacity.

27 Blau, J. (2006, May 26). Security Scores Big at World Cup Tournament. *PCWorld*. www.pcworld.com/article/125910/article.html

28 Genkin, D., et al. (2013). *RSA Key Extraction via Low-Bandwidth Acoustic Cryptoanalaysis*. www.cs.tau.ac.il/~tromer/acoustic

29 Gatto, K. (2011, May 31). The NutriSmart system would put RFIDs into your food for enhanced information. *PhysOrg.com*. phys.org/news/2011-05-nutrismart-rfids-food.html

metadata in order to build a social network graph of everyone who communicates digitally[30] as well as the full content of some 200 million text messages a day[31] (it is almost certain that other intelligence agencies attempt similar surveillance, but it is not yet documented publicly). Some countries have data retention laws that require ISPs to keep records of certain metadata, such as the sites that a user visits and their IP address, for up to seven years.[32] For a smaller country, however, it is entirely possible for a government to retain the content of communication as well, including all text messages and all phone conversations, using inexpensive commercially available equipment.

Third parties: All digital communication leaves a record with third-party intermediaries (except in special circumstances).[33] Third parties may include email providers, telephone carriers, ISPs, credit card companies, online retail, computer backup or file storage, and many mobile app developers (since many apps will store user data on the server). Much of the third-party tracking is carried out for the purpose of advertising and market research, some of which is visible, in the case of loyalty discount cards, while some is invisible to the user, such as ad targeting. Third-party advertising networks are able to track a user's internet behaviour, even when the user switches devices, because most websites and mobile applications use one or more of the same advertising and tracking networks. Although intended for commercial use, government surveillance agencies are able to use tracking data sent to advertising networks[34] and application data sent to computer servers[35] as a rich source of surveillance of personal information.

Digital surveillance grows up

Digital surveillance is still in its infancy. Governments collect more data than they know how to effectively process, facial recognition is still not accurate, and tracking databases are full of false information. For some, this is a comfort: no matter how much the surveillance net expands, it will be full of holes (and also false positives, with sometimes tragic personal results for those falsely convicted).[36]

Unfortunately, we are living in an age where the management and processing of information has become an essential component of industry, agriculture, public health, military, and soon education – in other words, nearly every aspect of state management and private business. These systems all need information to function, and surveillance designed to feed these systems more information is getting better all the time. Digital surveillance may be in its infancy, but it is working hard to grow up fast.

Despite the rather dire picture painted by this brief tour of digital surveillance, those who are concerned by the rapid maturation of surveillance and expansion into more aspects of social life have cause for hope. The struggle for the future of digital communication – who can control the flow of bits and who can assign identity to those bits – is being actively fought on the terrains of politics, law and technology. While all these terrains are important, new advances in the technology of encryption, usability and open protocols have the potential to offer powerful protection to the common user in the near future.

30 Greenwald, G., & Ackerman S. (2013, June 27). How the NSA is still harvesting your online data. *The Guardian*. www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

31 Ball, J. (2014, January 16). NSA collects millions of text messages daily in 'untargeted' global sweep. *The Guardian*. www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep

32 The Wikipedia page on data retention has the most up-to-date overview of the current state of retention laws around the world. https://en.wikipedia.org/wiki/Telecommunications_data_retention

33 It takes a very careful design to create a system that does not leak communication records to intermediaries. Even most peer-to-peer systems will leak relationship or timing information in the traffic. As of this writing, probably the most effective system designed to leave no useful information with intermediaries is a program called "Pond", although it is still experimental, hard to use, and has few users. See: https://pond.imperialviolet.org

34 Soltani, A., et al. (2013, December 10). NSA uses Google cookies to pinpoint targets for hacking. *Washington Post*. www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking

35 Ball, J. (2014, January 27). Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data. *The Guardian*. www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

36 Starr, G. (2014, June 26). What Your Cell Phone Can't Tell the Police. *The New Yorker*. www.newyorker.com/online/blogs/newsdesk/2014/06/what-your-cell-phone-cant-tell-the-police.html