Running head: BIG DATA AND INTELLIGENCE LED POLICING

Big Data, and Intelligence-Led Policing - A Comprehensive View

by Richard Bartel ID 0023717

University of Maryland, University College (UMUC), Spring 2018

CJMS 640 (9040), Week 12

April 15, 2018, Updated 5/5/2018

**Abstract**

The information and data sources for Intelligence led policing will likely evolve to include access to various forms of “big data”, raw and / or analyzed. Big data is attractive concept for those users who would like to divine a broader and certain reality in their pursuit of integrated systems, to support a more known and “efficient” world. Unfortunately, big data has reduced fidelity and increased high volume inefficiencies, particularly as data ages. (Chen, 2018). Even a pervasive police state would have inherent inefficiencies, bottlenecks of bureaucracy and data, significant errors, and false positives and negatives. This balancing has been the subject of popular cult films, such as “Brazil”. (Stivers, 2006). The author here concludes that big data uses, if incorporated into intelligence led policing at all, should be limited in its overlaps between traditional Intelligence and police operations. His reasons include the need to reduce the exposure of Intelligence and Police data to unauthorized access and uses, and to mitigate the compromise of information and privacy lost through hacked telecommunications systems (SS7, Diameter). Intelligence and Police should maintain a bicameral view of the world (including, keeping one eye on the other), and work together to prevent use of data by organized crime and totalitarian regimes (Daniels, 2018). The author suggests that Personally Identifiable Information (PII) related data be deleted, erased, and/or de-identified every 6-8 years, and that end to end encryption may go a long way in protecting data, devices, and networks.

**Introduction**

Intelligence led Policing data uses had their beginnings in “information ethics” at Oxford in the United Kingdom. The data sharing then between early Constabularies were based on professional relationships and trust. Recently, Information Technology (“IT”) ethics have described some undesirable methods of using data and related technologies. (Chatterjee, Sarker, & Valacich, 2015). Overall, the moral stewardship of keeping records has been studied with respect to Library science to this day. (Van Deer Ver Martens, 2017).

Now, however, law enforcement analysts are one of many hundreds of access points to common sources of information (such as what is provided to “fusion centers”). Access to such data centers are now commercially available through the internet, specifically designed for intelligence, police, and other governmental requirements. (i.e. Verint, Narus, and others). As with any “new” system, its growth will initially seem appealing for the common good. The marketers trumpet efficiency (Chen, 2018), and “progress”.

In general, Big Data has beget Cloud computing, which has renewed the need for “super” computers and development of Artificial Intelligence (AI). They are all touted as capable to assist the regulation of increasingly complex systems. Others will show that large data collections can become instrumental in describing and visualizing broad governmental, social, and medical issues which can be solved or improved.

For example, large data collections can improve operation of our power grid (Esri, 2018), a somewhat laudable project, but which might have also increased the grid’s cyber vulnerabilities, a known, but is left with unquantified and ill-defined major risks. Data can also assist organizations in the tracking and modeling of health and disease to develop public health responses and plans and programs. However, the collection and accumulation of data, as with all technology advances, inevitably will lead to behaviors which are considered immoral or unethical (such as hacking, software piracy, phishing, and spoofing (Dale, 2018)), and may involve other illegal and/or unconstitutional behaviors.

**Some Big Data Concerns**

When it comes to individual health, the collection and sharing of data has raised privacy concerns. (HIPPA at <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> ). In Europe, Privacy is one of many issues which has awakened a desire for General Data Protection Regulation. (Dale, 2018).

In addition, inevitably and ominously, “big data” now is becoming a pervasive and persistent source of information used for and deposited from electronic surveillance, to include facial recognition and tracking, addressed below. These technical tools have tended to attract “social engineers” to “…***nudge*** people to do things they otherwise might not do…”, or to persuade them to make personal changes more quickly than nature would have them accomplish in the due course of living their lives, which may be “sub-conscious”. These subtle pressures can induce significant fundamental personal changes, interfering with nature’s normal personal growth in individuals, which appears to catalyze in individual minds about every seven years (Bellman, 1978).

But, when does ‘nudge’ by social and political engineers come to “*shove*” ? One cultural example would be China, which I suggest might be one of numerous examples, which has formulated a “social credit system” (already in effect for volunteers, and required generally in 2020), to rate all citizens based on their “big data” and/or governmental information profile, where “citizens conforming to governmentally approved behaviors will earn a high numerical rating; nonconformists can expect unhappy consequences.” (Daniels, 2018).

In one sense, China’s experiment is the mirror image of predictive policing in the West. In China, the picture of an individual is planned to be partially drawn from surveillance, and the building of a record of “good works”. In the Western world the picture of an individual is gleaned from the record of what that individual has affirmatively been convicted of doing to breach the law, which records can be “expunged” on motion in Court if there are no recent crimes.

Thus, in the West, Intelligence Led Policing (ILP) tends to rely upon a layered criminal profiling. The problem in any culture is that there is no technical or political consensus about what is fresh data, what the weighting should be, and how long data should be reliable or usable. I propose that everyone would be better served if all individual data is considered stale and deleted, erased, and/or cleansed (de-identified), at least for Personally Identifiable Information (PII)), when the data is over 4 to 8 years old. (Bellman, 1978). The problem is that pattern analysis and recognition applied to massive databases (supplemented with artificial intelligence (AI), can lead to virtual “personally identifiable information”, which can be tracked and thus monitored.

The research indicates that behavioral psychology, biology, and ethics point to the need for social group behaviors to guide and inform rational governance strategy, rather than move policy based on individual actions. The society will be more just, and recognize the changes in behavior which individuals are naturally inclined to adopt as they mature. As indicated, study of natural human development and behavior has tended to confirm that such revival occurs naturally every 7 years. (Bellman, *supra*).

**Some current examples of possible unethical or illegal access to and uses of data**

A moral and just society should not permit the misuse of pervasive personal (PII) data by dictators, criminals, and organized crime. I have also suggested that there is a risk that intelligence led policing (ILP) access might be utilized for financial and/or other State proxy criminal activities. The Intelligence organizations and policing authorities of a society should counterbalance each other’s tolerance for unauthorized access to the data systems (i.e. fusion centers and internet based analogues). These problems appear to have been unassessed and are insufficiently addressed as a low occurrence, but high consequence risk.

For example, this issue may become a problem with small organizations or departments, particularly along national borders and/or financial centers. ILP data accesses, and attempts, should be tracked by reliable monitoring systems powered by valid and reliable artificial intelligence (AI) warning systems and pattern recognition capabilities. However the rise of cyber intrusion may not dissuade or protect individuals from unauthorized access, by government (and its proxies) and “industry”.

Data managers everywhere are scrambling to protect their data from the hacking, malware, ransomware and botnets. The data protection regulation near passage in the European Union could change the way many U.S. companies protect their data from inside and outside forces. For some U.S. companies doing business in Europe and preparing for compliance, the EU's General Data Protection Regulation could be a well-intended enforcer of better data governance practices broadly. (Tech Target, 2018, April).

**Intelligent Led Policing**

In the Western world, ILP Thus a layered terrorist profiling, based on a reliable big data methodology, is attractive to analysts. However, as I previously have written, data coordination was useful where terrorist actors were already well known data points for related crimes, spanning multiple countries. (National Review, 2015, May 4). For example, In the case of the Boston Marathon bombings, the actor was motivated to violence by an underlying ritualistic impulse, combined with a jihadist ideology in Chechen culture (Goltz, 2013). It was said that the Tsarnaev brothers and one other person, Ibragim Todashev… had also “..Likely ritually murdered three men, one of whom had been their friend”. (Perlmutter, D. 2013). Data may have been sufficient to detect a likely event, but the data was sporadic, distributed, and without alert criteria was not “actionable”.

**Compromised Telecommunications Systems**

As for data abuses, there exists new information that data within the world’s telecommunications systems (including cellphone and such devices), has been used routinely by governments, private security firms, and intelligence agencies to essentially hack into the tracking and derivative data on almost all phone and network users, based only on their phone numbers. Even an iPad has a phone number internally. It has been reported that there is a race to index one’s telephone number to locate surveillance baselines with regard to individuals, with the U.S. National Security Agency (NSA) tripling its attention to phone numbers since 2017, scooping up 534 million communications in bulk. (Vinograd, 2018).

There are also surveillance methods which track devices by their MAC Address, and device (Integrated Circuit Card Identifier (IMSI “IMSI catchers”)). In another system, the U.S. FBI’s and local police use its “Stingray” program sits on the periphery with “fake” cell phone towers pinging devices for location and other data), such as information on IMSI related “SIM” chips. The device’s - International mobile Subscriber Identity (ICCID) identifies SIMs internationally, spurning millions of “fake” SIMs being sold internationally on the Web. IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network). (<https://www.quora.com/What-is-the-difference-between-ICCID-IMSI-and-IMEI-numbers> ). IMSI is one of the indexes now used to track devices and trick billing systems.

The media access control address (“MAC”) is usually hard coded in each device Input or Output system (i.e. modems, LAN connections, WiFi transceivers, and other emissions, and there are legal captions where the MAC address is the Defendant’s alias, such as when tracking a laptop, desktop, or iPad). (<https://www.google.com/imgres?imgurl=https://upload.wikimedia.org/wikipedia/commons/thumb/9/94/MAC-48_Address.svg/475px-MAC-48_Address.svg.png&imgrefurl=https://en.wikipedia.org/wiki/MAC_address&h=400&w=475&tbnid=BJcXcirlmXehdM:&tbnh=160&tbnw=190&usg=__TXZkI_3h0Lz_TxgAdCJ_TVY1Cps%3D&vet=1&docid=o5g_SweFRPHepM&client=firefox-b-1&sa=X&ved=0ahUKEwichZm24-7aAhWhmuAKHaJkAZEQ9QEIKzAA> ).

As I have indicated, even the phone number alone enables one to at least track every device, worldwide. The alleged extra judicial tracking is real time for locations and movements worldwide, using inherent systemic flaws in the SS7 and Diameter telephone switching and identifications systems, and that data is now available for commercial “intelligence-led policing” and Intelligence products for sale to anyone willing to pay for access. (FCC advisory committee, Communications Security, Reliability, and Interoperability Council (CSRIC, 2018). For illustration, there are many data access companies which are offering at least some of such tracking capabilities (i.e. Verint (as identified by German researchers), and Narus, recenltly acquired by Boeing and then Symantec (2015)). (<https://www.forbes.com/sites/greatspeculations/2015/01/14/symantec-acquires-boeings-cybersecurity-unit-in-a-bid-to-boost-big-data-capabilities/#1dca9d1a7ec3> ), which allegedly have current or past Israeli influences or designs. (Some additional discussion at Appendix A herein).

Government has also found value in using the telecommunications identifiers noted above, allegedly for focused investigations, but recent press has indicated that unauthorized similar tracking is being used intensely by numerous known and unknown domestic and foreign intelligence organizations, particularly in and around Washington, D.C. (2018). Once operationally in “the wild” , it may be a short step for similar uses by organized crime, to manage its own operations and monitor police activity. More basic local data is collected by car license tag reader data compiled and processed for video tracking on streets and highways. In Virginia, the State’s Supreme Court has ruled that a suit against the Fairfax County police department regarding retention of tag reader data could proceed. (Neal v Fairfax County Police Department , April 26, 2018).

Also, Quoting the Federal Communications Commission (FCC) advisory committee (CSRIC) Working Group 3, Network Reliability and Security Risk Reduction Final Report – Recommendations to Mitigate Security Risks for Diameter Networks, Version 1.1 – March 14th 2018, is found below in *Appendix A, Compromised Telecommunications***.**

It is possible that these methods at compromising telecommunications networks are increasing in use by governments, intelligence, and police, and now that internet based accesses are for sale, and not unexpectedly there are likely efforts underway for other actors to use the same vulnerabilities and exploits to serve criminal and commercial requirements and abuses.

These revelations show that Intelligence agencies, and now criminal organizations or nation state proxies, have little reservation in using and exploiting crucial inherent data sources to obtain national intelligence operational products, where police would not likely be authorized to do so. This shows that there is a necessity for a firewall between Intelligence and Policing, and thus I have recommended the maintenance of the traditional “bicameral view) of Intelligence and Policing, as crucial to our civil liberties.

**Compromising Manufacturer and Network software update action or inactions (See Appendix B)**

If these data misuses are not enough, there is evidence that devices (such as Android phones) are not being updated as they pretend to be by carriers or manufactures. A study released in April, 2018, indicates that Android phones aren't just slow to get patched, but sometimes manufacturers and carriers are lying about being patched, when they're actually not being updated. (Nohl & Lell, 2018). As published from Security Research Labs in WIRED Magazine (2018, April 12), see below in **Appendix B**.

**Conclusions**

The information and data sources for Intelligence led policing will likely evolve to include access to various forms of “big data”, raw and / or analyzed. Big data is an attractive concept for those users who would like to divine a broader and certain reality in their pursuit of integrated systems, to support a more known and “efficient” world. Unfortunately big data has reduced fidelity and high volume inefficiencies, particularly as data ages. (Chen, 2018).

Even a pervasive police state would have inherent inefficiencies, bottlenecks of data, significant errors, and false positives and negatives. This balancing of technology, process, and terrorism has even been the subject of popular cult movies, such as “Brazil”. (Stivers, 2006).

I conclude that big data, if incorporated into intelligence led policing at all, should be limited in its overlap with traditional Intelligence operations. There is an unassessed general risk that law enforcement and intelligence operatives are only two of many hundreds of access points to common sources of information (such as what is provided to “fusion centers”). Access to such data centers are now commercially available through the internet, specifically designed for intelligence, police, and other governmental requirements.

Recent revelations of abuses with worldwide data and router vulnerabilities abound. These revelations show that Intelligence agencies and commercial entities have little reservation in using and exploiting crucial inherent data sources to obtain national intelligence operational products, where police would not likely be authorized to do so.

The author proposes that Intelligence and Policing also should have only nominal overlaps in order to maintain a bicameral view of the world (including, keeping one eye on the other), and prevent use by organized crime and totalitarian regimes (Daniels, 2018). The author suggests that Personally Identifiable Information (PII) related data be deleted, erased, or de-identified every 6-8 years from all databases. This should mitigate a large part of accumulating Privacy issues.

These revelations show that Intelligence agencies, and now criminal organizations or nation state proxies, have little reservation in using and exploiting crucial inherent data sources to obtain national intelligence operational products, where police would not likely be authorized to do so. This shows that there is a necessity for a firewall between Intelligence and Policing, and thus I have recommended the maintenance of the traditional “bicameral view) of Intelligence and Policing, as crucial to our civil liberties.

**References**

… Esri. (2018, Spring). “Big data keeps the lights on, monitoring and maintaining the US power grid relies on real-time geo-visualizations”. ArcNews, Vol 40, Iss 2, p 1

Bellman, G. (1978, Nov). Passages: Predictable Crises of Adult Life. Training & Development Journal, Vol. 32, Iss 11, pp 49-53. Also see: Sheehy, Gail.

Chatterjee, S, Sarker, S, & Valacich, J. (2015, Spring). “The behavioral roots of information systems security: exploring key factors related to unethical IT use”. *Journal of Management Information Systems*, Vol 31 Iss 4, p 49-87. doi: 10.1080/07421222.2014.1001257

Chen, A. (2018, April 12). “Why trying to be too efficient will make us less efficient in the long run, Edward Tenner explains the efficiency paradox”. Retrieved April 15, 2018 from https://www.theverge.com/2018/4/12/17229158/edward-tenner-efficiency-paradox-big-data-artificial-intelligence-book

Dale, S. (2018, March). New data protection regulations. Therapy Today, Vol 29, Iss 2, p 50. MEDLINE ID 101261681, ISSN 1748-7846.

Daniels, M. (2018, March 28). “Big data is always watching”. The Washington Post; Mitch Daniels as President of Purdue University, and former Governor of Indiana.

FCC Communications security, reliability, and Interoperability Council. (2018), retrieved from <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council>

Goltz, T. (2013, May 13). The Chechen connection. Nation, Vol 296, Iss 19, pp 8-10.

Michaels, C. W. (2002). “No greater threat: America after September 11 and the rise of a national security state”. Algora publishing. ISBN 0-87586-154-7

Nohl, K & Lell, J. (2018, April 12). How Android phones hide missed security updates from you. Security Research Labs, WIRED Magazine, Greenberg, M (Ed.). Retrieved from <https://www.wired.com/story/android-phones-hide-missed-security-updates-from-you/>

National Review. (2015, May 4). Vol. 67 Issue 8, 4

Perlmutter, D. (2013, Fall). Prelude to the Boston bombings. Middle East Quarterly, Vol. 20, Iss 4, pp 67-77

Puzankov, S & Kurbatov, D. (2014, May 27). “How to intercept a conversation held on the other side of the planet”. Positive Technologies. Retrieved from [https://www.slideshare.net/phdays/phd4-pres-callinterception119 4/15/2018](https://www.slideshare.net/phdays/phd4-pres-callinterception119%204/15/2018). [spuzankov@ptsecurity.com](mailto:spuzankov@ptsecurity.com) , [dkurbatov@ptsecurity.com](mailto:dkurbatov@ptsecurity.com) .

Reith, E. (2011). Purchase wireless collection , technology and non-disclosure obligations. c/o Tracking Technology Unit, Bldg 27958A, Pod B, Quantico, VA 22135, 703-985-2608. Referring to Harris Corporation, as applied to Baltimore, Maryland police. Retrieved from public internet at <http://www.documentcloud.org/documents/1808819-baltimore-police-stingray-non-disclosure-agreement.html> ). May 5, 2018.

Stivers, R. (2006). “Technology and terrorism in the movie Brazil”. Bulletin of Science, Technology and Society, Vol. 26, Iss 1, p 20-22 . Retrieved from <http://journals.sagepub.com/doi/abs/10.1177/0270467605284343> .

Van Der Veer Martins, B. (2017). New grounds for ontic trust: information objects and LIS. Education for Information, Vol 33, Iss 1, p 37-54. doi: 10.3233/EFI-170988

TechTarget . (2018, April). Security of bid data fashions a whole new look for GDPR. Vo 6, Iss 2. Retrieved from: [https://searchdatamanagement.techtarget.com/ezine/Business-Information/Security-of-big-data-fashions-a-whole-new-look-with-GDPR?track=NL-1815&ad=920282&src=920282&asrc=EM\_NLN\_93359563&utm\_medium=EM&utm\_source=NLN&utm\_campaign=20180410\_Europe%20to%20strong- arm%20U.S.%20into%20better%20data%20protection,%20blockchain%20payroll%20in%20the%20works,%20AI%20to%20improve%20demand%20forecasting,%20and%20more](https://searchdatamanagement.techtarget.com/ezine/Business-Information/Security-of-big-data-fashions-a-whole-new-look-with-GDPR?track=NL-1815&ad=920282&src=920282&asrc=EM_NLN_93359563&utm_medium=EM&utm_source=NLN&utm_campaign=20180410_Europe%20to%20strong-%20arm%20U.S.%20into%20better%20data%20protection,%20blockchain%20payroll%20in%20the%20works,%20AI%20to%20improve%20demand%20forecasting,%20and%20more)

Vinograd, S. (2018, May 5). Phone number surveillance. CNN.

**APPENDIX A – Compromised Telecommunications**

“As described in the CSRIC V Working Group 10 Report, while the overwhelming majority amount of traffic using the Signaling System 7 (SS7) protocol is legitimate, the SS7 network connecting hundreds of wireless networks globally is subject to potential exploitation by bad actors that improperly obtain valid credentials on the black market. Current research indicates that similar vulnerabilities demonstrated in SS7 networks may also apply to Diameter networks, used in 4G/LTE as well as AIN/charging networks.

The use cases found in SS7 may exist in Diameter as well, namely: location tracking; voice/SMS interception; subscriber denial of service (DoS); and account fraud/modification. In addition to these use cases, the Diameter protocol may be used for the interception of user data sessions. Previous research exposed the GPRS Tunneling Protocol (GTP) to be vulnerable in 3G networks, but the functions provided by GTP have been replaced by the Diameter protocol in 4G. The Diameter protocol also introduces the potential to spoof the identity of networks due to the way Diameter routes commands from hop-to-hop, which is unique to Diameter. Similar to SS7, nation state attacks are believed to be the largest threat, and such attackers can be highly sophisticated and well-funded.

The Diameter vulnerabilities are at the same stage that SS7 was at just a few years ago. While the research community has begun to demonstrate use cases that can be used to exploit Diameter vulnerabilities, few if any attacks have been identified in production networks to date. This can be attributed to the fact that Diameter is not widely deployed between networks today and that the vulnerability (as with SS7) is tied to roaming. Carriers have not, to date, entered into widespread LTE roaming agreement and, as such, attackers continue to focus on SS7. As LTE roaming becomes more prevalent, this may change and the industry will be ready to meet the threat.

Due to the similarities between SS7 and Diameter threats, the industry can use the successful “playbook” it employed to combat SS7 threats to protect Diameter.1 These steps, which are further delineated in the recommendations in this report, include: blocking certain message types, as recommended by GSMA; employing monitoring platforms; and implementing advanced firewalls. The industry has already begun these efforts, well before wide-spread targeting of Diameter by nefarious intruders.

Specifically, mitigation includes the implementation of firewall rules and policies deployed at the network edge (implementation of such can be through a standalone firewall appliance or Diameter edge agent, or DEA). The GSMA has documented guidelines for defining these rules and policies in FS.19 and FS.21. The GSMA continues work on these guidelines and should be the principal reference for safeguarding networks.

The SS7 interface (connecting to the network Home Subscriber Server, or HSS) is the first focus of any security plan and should be protected from outside abuse. There are other interfaces providing external access to network resources that should be protected as well, but the S6a provides access to Personally Identifiable Information (PII) and network specifics, making it the prime target of attacks.

Following the release of the WG10 report in March 2017, the FCC encouraged carriers to implement the best practices recommended in the report, and industry publicly expressed support of the recommendations and noted that industry is implementing them.

Security zones should be implemented to ensure the vulnerabilities are containerized, and access to one domain in the network does not expose the entire network. Isolation of the DEA is one example of creating security zones.

Diameter networks can be protected, and in many cases there are much better tools for securing Diameter networks. This is perhaps one reason global operators are moving their interconnections to Diameter, in place of SS7. However, Diameter also introduces unique vulnerabilities that must be taken into consideration prior to implementing Diameter at the roaming interconnect.

Government, including the Department of Homeland Security (DHS), should continue to engage with industry about enhanced protections for certain government officials and potentially valuable targets. This may also include the use of commercially available media encryption technologies to secure their voice and data sessions.

In North America, there should be consideration given towards establishing a ‘Circle-of-Trust’ between operators, to help protect North American networks. Operators should work in collaboration towards this goal.

The industry should continue working with industry and standards organizations and adopt best practices and guidelines (such as those recommended by the GSMA) for Diameter security as part of their planning for 5G and IoT deployments. Further study will be needed for 5G specific security recommendations.” (File: csric6WG3\_finalreport32018.pdf). Found at https://www.fcc.gov/files/csric6wg3finalreport32018pdf ).

**Appendix B: Compromising telecommunications manufacturers and carriers update fraud**

“Google has long struggled with how best to get dozens of Android smartphone manufacturers—and hundreds of carriers—to regularly push out security-focused software updates. But when one German security firm looked under the hood of hundreds of Android phones, it found a troubling new wrinkle: Not only do many Android phone vendors fail to make patches available to their users, or delay their release for months; they sometimes also tell users their phone's firmware is fully up to date, even while they've secretly skipped patches.

On Friday at the Hack in the Box security conference in Amsterdam, researchers Karsten Nohl and Jakob Lell of the firm Security Research Labs plan to present the results of two years of reverse-engineering hundreds of Android phones' operating system code, painstakingly checking if each device actually contained the security patches indicated in its settings. They found what they call a "patch gap": In many cases, certain vendors' phones would tell users that they had all of Android's security patches up to a certain date, while in reality missing as many as a dozen patches from that period—leaving phones vulnerable to a broad collection of known hacking techniques.

"We find that there's a gap between patching claims and the actual patches installed on a device. It’s small for some devices and pretty significant for others," says Nohl, a well-known security researcher and SRL's founder. In the worst cases, Nohl says, Android phone manufacturers intentionally misrepresented when the device had last been patched. "Sometimes these guys just change the date without installing any patches. Probably for marketing reasons, they just set the patch level to almost an arbitrary date, whatever looks best."

The Patch Gap: SRL tested the firmware of 1,200 phones, from more than a dozen phone manufacturers, for every Android patch released in 2017. The devices were made by Google itself as well as major Android phone makers like Samsung, Motorola, and HTC, and lesser-known Chinese-owned companies like ZTE and TCL. Their testing found that other than Google's own flagship phones like the Pixel and Pixel 2, even top-tier phone vendors sometimes claimed to have patches installed that they actually lacked. And the lower-tier collection of manufacturers had a far messier record.

Sometimes these guys just change the date without installing any patches. The problem, Nohl points out, is worse than vendors merely neglecting to patch older devices, a common phenomenon. Instead, it's that they tell users they install patches that they in fact don't, creating a false sense of security. "We found several vendors that didn’t install a single patch but changed the patch date forward by several months," Nohl says. "That’s deliberate deception, and it's not very common."

More often, Nohl believes, companies like Sony or Samsung would miss a patch or two by accident. But in other cases, the results were harder to explain: SRL found that one Samsung phone, the 2016 J5, was perfectly honest about telling the user which patches it had installed and which it still lacked, while Samsung's 2016 J3 claimed to have every Android patch issued in 2017 but lacked 12 of them—two considered as "critical" for the phone's security.

Given that kind of hidden inconsistency, "it's almost impossible for the user to know which patches are actually installed," Nohl says. In an effort to solve that missing patch transparency problem, SRL Labs is also releasing an update to its Android app SnoopSnitch that will let users check their phone's code for the actual state of its security updates.

A Patchwork of Patching Practices: After averaging out the results of every phone tested for each vendor, SRL labs produced the chart below, which splits vendors into three categories based how faithfully their patching claims matched reality in 2017, focusing only on phones that received at least one patch in October of 2017 or later. Phones from major Android vendors including Xiaomi and Nokia had on average between one and three missing patches, and even major vendors like HTC, Motorola, and LG missed between three and four of the patches they claimed to have installed. But the lowest-performing companies on the list were the Chinese firms TCL and ZTE, all of whose phones had on average more than four patches that they'd claimed to have installed, but hadn't.

SRL also points to chip suppliers as one possible reason for missing patches: While phones with processors from Samsung had very few silently skipped patches, ones that used chips from the Taiwanese firm MediaTek lacked a whopping 9.7 patches on average. That may in some cases be simply because cheaper phones are more likely to skip patches, and also tend to use cheaper chips. But in other cases, it's because bugs are found in the phone's chips rather than in its operating system, and the phone manufacturer depends on the chipmaker to offer a patch. As a result, cheaper phones that source chips from lower-end suppliers inherit those suppliers' missed patches. "The lessons is that if you go for a cheaper device, you end up in a less well maintained part to this ecosystem," Nohl says.

When WIRED reached out to Google, the company said that it appreciated SRL's research, but responded by pointing out that some of the devices SRL analyzed may not have been Android certified devices, meaning they're not held to Google's standards of security. They noted that modern Android phones have security features that make them difficult to hack even when they do have unpatched security vulnerabilities. And they argued that in some cases, patches might have been missing from devices because the phone vendors responded by simply removing a vulnerable feature from the phone rather than patch it, or the phone didn't have that feature in the first place. The company says it's working with SRL Labs to further investigate its findings. "Security updates are one of many layers used to protect Android devices and users," added Scott Roberts, Android product security lead, a statement to WIRED. "Built-in platform protections, such as application sandboxing, and security services, such as Google Play Protect, are just as important. These layers of security—combined with the tremendous diversity of the Android ecosystem—contribute to the researchers' conclusions that remote exploitation of Android devices remains challenging."1

In response to Google's assertion that some patches may have been unnecessary due to the vulnerable feature being missing from the phone or removed in response to the vulnerability, Nohl counters that those situations very rare. "It’s definitely not a significant number," he says.

Not the Lowest Hanging Fruit: More surprisingly, Nohl agrees with Google's other major point: Hacking Android phones by exploiting their missing patches is far harder than it sounds. Even Android phones that don't have solid patching records still benefit from Android's broader security measures, like address space layout randomization—which since Android 4.0 (Lollipop) has randomized the location of a program in memory to make it harder for malware to exploit other parts of the phone—and sandboxing, which limits a malicious program's access to the rest of the device.

That means most hacking techniques, known as exploits, that can gain full control of a target Android phone requires taking advantage of a series of vulnerabilities in a phone's software, not just one missed patch. "Even if you miss certain patches, chances are they’re not aligned in a certain way that allows you to exploit them," Nohl says.

As a result, he says, Android phones are far more often hacked with simpler schemes, namely rogue apps that find their way into the Google Play Store or that trick users into installing them from other sources outside of the Play Store. "Criminals will most likely stick with social engineering as long as humans are gullible and install free or pirated software that comes packaged with malware," Nohl says.

Advanced, state-sponsored hackers carrying out more targeted attacks on Android devices, however, may be another story. For the most part, Nohl argues they likely use zero-day vulnerabilities—secret hackable bugs for which no patch exists at all—rather than known but unpatched vulnerabilities. But in many cases they might use known and yet unpatched bugs in phones in combination with zero day vulnerabilities; he refers, as an example, to the spyware FinFisher, which at one point took advantage of a known Android vulnerability called Dirty COW in addition to its own fresh zero-day exploits.

Nohl cites the security principle of "defense in depth"—that security is most effectively implemented in multiple layers. And every missed patch is potentially one less layer of protection. "You should never make it any easier for the attacker by leaving open bugs that in your view don’t constitute a risk by themselves, but may be one of the pieces of someone else's puzzle," Nohl says. "Defense in depth means install all the patches." (WIRED, April 12, 2018).

Nohl, K & Lell, J. (2018, April 12). Security Research Labs, WIRED Magazine, Greenberg, M (Ed.). Retrieved from https://www.wired.com/story/android-phones-hide-missed-security-updates-from-you/Karsten Nohl and Jakob Lell of the firm Security Research Labs.

Appendix C: Some recent Intelligence operations

The UKUSA Agreement is an agreement between the United Kingdom, United States, Australia, Canada, and New Zealand to cooperatively collect, analyze, and share intelligence. Members of this group, known as the “Five Eyes”, focus on gathering and analyzing intelligence from different parts of the world. While Five Eyes countries have agreed to not spy on each other as adversaries, leaks by Snowden have revealed that some Five Eyes members monitor each other’s citizens and share intelligence to avoid breaking domestic laws that prohibit them from spying on their own citizens. The Five Eyes alliance also cooperates with groups of third party countries to share intelligence (forming the Nine Eyes and Fourteen Eyes), however Five Eyes and third party countries can and do spy on each other. (Source <https://privacytools-io.github.io/> ).

Five Eyes 1. Australia 2. Canada 3. New Zealand 4. United Kingdom 5. United States of America

Nine Eyes: 6. Denmark 7. France 8. Netherlands 9. Norway

Fourteen Eyes 10. Belgium 11. Germany 12. Italy 13. Spain 14. Sweden