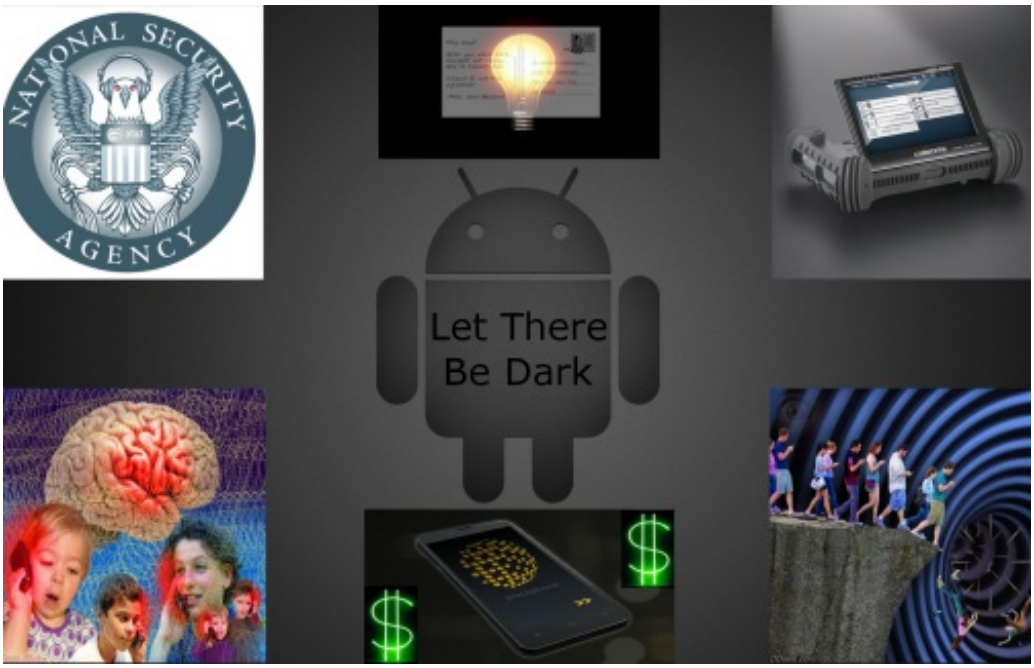
Are Cellular Telephones Furthering Human Liberty?

www.thelastbastille.com/2016/06/06/cellular-telephones-furthering-human-liberty/

"Can you remember a time when you went for a walk or out to the shops or even commuted home to and from your job without the need to carry around a mobile phone? Today's phones feature GPS tracking, wireless network hookup and even allow Google the knowledge of your exact physical location for improved search and 'other services.' We have sold the freedom of privacy, friends, and in attempting to avoid ever being alone again we have isolated ourselves by becoming enslaved to our gadgets…[s]o here we are, suckered into thinking we are in communication with others at all times, yet limiting ourselves in actual ability to communicate clearly by crippling the English language in order to save time on sending text messages. Save time for what? More World of Warcraft?"

– The Anti-Terrorist



Introduction

Technology is a double-edged sword. It can be used for good ends, but it also be used to commit unspeakable evil. Whether it is used for one or the other ultimately depends on the choices that are made by individuals. Understanding how any technology works is pivotal in exercising free will by way of making informed choices.

Shane Radliff has recently discovered that it is indeed possible to browse the Internet and talk anonymously using cellular telephones. This is chiefly accomplished through buying prepaid mobile phones, activating them using as little personally identifiable information (PII) as possible, and then configuring them with smartphone apps that encrypt both text and voice communications using digital encryption protocols like Off-the-Record (OTR) and the Zimmerman Real-Time Protocol (ZRTP). Developments in the on-going crypto wars will reveal over time whether free and open-source software, as used by the people, have an indispensible role in preventing the deciphering of digitally encrypted material by the government's cryptanalysts.

Personally, I think the more fundamental question revolves around whether cell phones are mostly beneficial or

noticeably detrimental to individual liberty. Security culture is only valuable to the extent that its practitioners are less vulnerable to coercion than those who fail to take their right to privacy seriously. Weighing both the pros and cons of cell phone ownership necessarily entails a thorough grounding as to how such an invention has a multi-faceted significance within your own life.

Search Warrants, Fourth Amendment "Papers," & Color of Law

Any constitutionalist worth their salt knows that the Fourth Amendment's Warrant and Search & Seizure Clauses are the legal protections against indiscriminate surveillance, including dragnet wiretapping. While the right to privacy is not enumerated like the right to keep and bear arms or the right of peaceful assembly, the constitutional limits upon searches, seizures, and the issuance of warrants did inadvertently value individual privacy. Unfortunately, the federal judiciary's constitutional interpretations of the Fourth Amendment are typically weighed against the citizenry, especially when cellular telephones are at play.

In 2006, Judge Lewis Kaplan's memorandum opinion in *United States v. Tomero, et. al.*, under the auspices of the United States District Court for the Southern District of New York, ruled that the FBI's installation of roving wiretap bugs in the defendants' cell phones were not unconstitutional. Six years later, Judge Richard Posner wrote the United States Court of Appeals for the Seventh Circuit's decision in *United States v. Abel Flores-Lopez* that a warrantless search of the defendant's cell phone in order to verify the cell phone's number was not a violation of the Fourth Amendment. Five months later in 2012, Judge Raymond Fisher conveyed the federal appellate's Ninth Circuit decision in *United States v. Ortiz Oliva* that the electronic surveillance orders only authorized "standard interception techniques," and therefore did not convert the defendant's cell phone into a roving wiretap, despite the self-evident fact that the police, indeed, turned the phone into a roving wiretap.

About a month later in August of 2012, Judge John Rogers delivered the opinion of the U.S. Court of Appeals for the Sixth Circuit in *United States v. Melvin Skinner*, which ruled that the defendant's lack of knowledge about his cell phone's geolocation capabilities did not give him an expectation of privacy, especially against police surveillance. In both May and August of 2013, the United States District Court for the District of Arizona's Judge David Campbell repeatedly decided that the 2008 Tracking Warrant for the defendant's cell phone did not violate the Fourth Amendment since the aircard was bought by way of identity theft, according to these court documents from the *United States v. Daniel Rigmaiden* case. On January 11th of 2016, the United States Supreme Court denied a petition for a writ of certiorari in the *EPIC v. DHS* case, which was all about whether or not the federal government possessed an Internet kill switch that would also simultaneously shut down cellular towers during the onset of a government declared emergency.

Whether the specific issues of these half dozen federal court cases dealt with roving wiretap bugs, geolocation, kill switches, defective warrants, or warrantless searches of the cell phones themselves, these federal judges consistently ruled against the defendants' right to privacy, largely on the presumption that accused criminals have no expectation of privacy, even if they were engaging in "criminally victimless" activity. The bugging of a defense lawyer's cell phone in the 2006 *Tomero* case is particularly troubling, for Judge Kaplan explained that:

> *"By February 2004, the government had learned that Peter Peluso, an attorney and close associate of Ardito, was relaying messages to and from high-ranking family members who were wary of government listening devices and who used Peluso as a messenger to avoid meeting together directly. In a renewal application dated February 6, 2004, the government sought, and Judge Jones in due course granted, authority to install a roving bug in Peluso's cellular telephone. This order was renewed several times throughout 2004, as the government continued to identify locations where*

> *Peluso and Ardito discussed family matters and learned that the subjects were growing increasingly cautious of government surveillance.*
>
> *"In January 2005, Peluso agreed to cooperate with the government's investigation. At that point the government removed the listening device in his cellular telephone and Peluso began recording conversations with family members consensually by wearing a microphone. On July 7, 2005, Peluso pleaded guilty, pursuant to a cooperation agreement with the government, to a four-count information, charging him with, among other things, engaging in a pattern of racketeering activity."*

So, much for attorney-client privilege, huh? Notice also that Peluso turned state's evidence 11 months after the roving bug was placed, most likely after the government police Bluecoats informed him of what they had on him in terms of criminal charges and the harshness of the maximum sentence. Just as soon as Peluso had betrayed his clients, only then was the roving bug in his cell phone removed to then be replaced by a wire that he wore on his person.

I guess that if an investigative journalist was working a story and then accused by the government for anything, then the only way he could still work on the story would be to become an indentured serf for the prosecutor; whether the "professional" under the thumb of the government be an attorney or a journalist, you would think a possible legal defense against this practice would be for the defendant's counsel to issue a Fifth Amendment self-incrimination challenge, but unfortunately, such was not argued here in the *Tomero* case. In the 2012 *Flores-Lopez* case, Judge Posner wrote:

> *"In some cases, a search of a cell phone, though not authorized by a warrant, is justified by police officers' reasonable concerns for their safety. One can buy a stun gun that looks like a cell phone… [b]ut the defendant's cell phone, once securely in the hands of the arresting officer, endangered no one. It did, however, contain evidence or leads to evidence – as the officers knew was likely because they knew from their informant that as is typical of drug dealers the defendant had used cell phones to talk to Santana-Cabrera and other coconspirators. But was there any **urgency** about searching the cell phone for its phone number? Yet even if there wasn't, that bit of information might be so trivial that its seizure would not infringe the Fourth Amendment."*

What kind of pabulum is this? Apparently, the cult of "officer safety" still had ardent believers who impose their faith within secular courtrooms. Judge Posner continually draws on previous court case precedent:

> *"So, opening a diary found on the suspect whom the police have arrested, to verify his name and address and discover whether the diary contains information relevant to the crime for which he has been arrested, clearly is permissible; and what happened in this case was similar but even less intrusive, since a cell phone's phone number can be found without searching the phone's contents, unless the phone is password-protected – and some cell phones even if it is…[i]t's not even clear that we need a rule of law specific to cell phones or other computers. If police are entitled to open a*

> *pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number."*

Last time I checked, the Fourth Amendment applied to the people's "persons, houses, papers, and effects." **If a diary does not count as one's "papers," then what does?** Judge Posner finally concluded that a cost-benefit analysis by the police Bluecoats would not be feasible to do prior to searching a suspect under arrest. According to the 2012 *Oliva* ruling, Judge Fisher said:

> *"The 'off the hook' language, however, lacks meaning when applied to cellular phones. Terminating a call on a cellular phone does not turn the phone completely off. To do so requires a separate and more deliberate step that the user may not appreciate is necessary, and may leave the cellular phone open to electronic eavesdropping quite different from what can occur with accidentally failing to hang up a land line phone. Unlike a relatively stationary land line phone, a cellular phone whose microphone remains on even though the call is terminated becomes a truly 'roving bug.' If that is what the government's application for a warrant actually seeks, it cannot do so using arcane, outmoded terminology like 'off the hook.' "*

Whether we're talking about roving bugs or roving wiretaps (pursuant to the Omnibus Crime Control & Safe Streets Act of 1968), the fact of the matter is that Oliva's motion to suppress the evidence collected under the guise of a dubious warrant was denied. Judge Rogers, in the 2012 *Skinner* case, wrote:

> *"There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone. If a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal. The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools. Otherwise, dogs could not be used to track a fugitive if the fugitive did not know that the dog hounds had his scent. A getaway car could not be identified and followed based on the license plate number if the driver reasonably thought he had gotten away unseen. The recent nature of cell phone location technology does not change this. If it did, then technology would help criminals but not the police. It follows that Skinner had no expectation of privacy in the context of this case, just as the driver of a getaway car has no expectation of privacy in the particular combination of colors of the car's paint."*

It would seem to be the case that Judge Rogers thinks that technological ignorance (or even illiteracy) does not justify the defendant's expectation of privacy, because he equated the cell phone's GPS signaling to tracking hounds and getaway cars as the mere tools of both the police and the "criminals" they apprehend, respectively. Interestingly enough, this concept was explained more in depth by Judge Campbell in the 2013 *Rigmaiden* case; according to

the May 8th court order:

> *"One who so thoroughly immerses himself in layers of false identities should not later be heard to argue that society must recognize as legitimate his expectation of privacy in the location and implements of his fraud…[d]efendant did not have an expectation of privacy society is willing to accept as legitimate."*

So, the tools used by defendants and the government are fair game, unless the defendant is being accused by the prosecutor of acquiring those tools through fraud. Either way, the **defendants have no expectation of privacy**, regardless of whether they "voluntarily procured" their own tools, or acquired them fraudulently. In other words, if the government charges you with a crime, then your right to privacy will be infringed upon.

Underlying all of this jurisprudence is the color of law being committed by these judges, as well as the inevitable consequence that is the fruit of the poisonous tree. The origin of this seems to be a case that was frequently cited in *Tomero*, which was the 1993 *United States v. L Bianco* case that was decided by the federal Court of Appeals for the Second Circuit. Judge George Pratt wrote for the appellate panel (referring to a home that was used to conduct a ritualistic ceremony), saying:

> *"Since none of the defendants had any legitimate interest in the privacy of the 34 Guild Street residence before they arrived there, they lack standing to assert that the entry to install listening devices inured their rights."*

Now, by examining some references in *Tomero*, I think the "fruit" of legitimizing the roving bugs & roving wiretaps becomes rather apparent:

> *"Defendants point first to the fact that the order in **Bianco** authorized the placement of listening devices only in buildings whereas the order here authorized placement in mobile telephones. But the argument misses the point.*
>
> *"The essence of the motion to suppress is that the statute unconstitutionally permits interception in the absence of any specification of the place where communications are to be intercepted. In **Bianco**, the Second Circuit rejected precisely this argument. The fact that the unspecified location in **Bianco** happened to be in a building had nothing to do with the holding. Furthermore, while a mobile device makes interception easier and less costly to accomplish than a stationary one, this does not mean that it implicates new or different privacy concerns. It simply dispenses with the need for repeated installations and surreptitious entries into buildings. It does not invade zones of privacy that the government could not reach by more conventional means."*

Well, there's your common law for you. The *Tomero* defendants' as-applied challenge was rejected by the court, even though there is a substantive difference between wiretapping a cell phone and bugging a room, as the later was the case in *Bianco*; this set the stage for the successful prosecution of the *Oliva* defendants, because the precedent had already been laid by *Bianco* and *Tomero*.

Something not too dissimilar could be said about warrantless searches and geolocation. The color of law here would seem to begin with *Flores-Lopez*, "just" for the purpose of warrantlessly "validating" the defendant's cell number, which would be considered metadata. Later in *Skinner*, actively tracking the cell phone remotely was warrantlessly permissible because the defendant wasn't careful enough in disabling the geolocation feature. This set the stage for *Rigmaiden*, where the fruit of the poisonous tree ripens, which is all thanks to Judge Campbell's interpretation that the warrant was valid because the defendant was suspected of using his fraudulently acquired tools to commit more crimes (this would be comparable to a presumption that if you did not have your return address on a letter, then the Bluecoats could just assume nefarious activity and then proceed to open your mail). The similarity between *Flores-Lopez*, *Skinner*, & *Rigmaiden* is that although there was no wiretapping as in the other trio of aforementioned cases, the remote tracking as well as the physical search & seizure of the cell phones in question was tipped heavily in favor of the prosecutor, based on the assumption that the mere "suspicion" of "criminal" activity "suspends" the defendant's right to privacy, and by extension, due process as well.

What are the implications of all this judicial precedent? It would appear to be the case that the issuance of what historically would be considered to be general warrants (more specifically, the historical writs of assistance opposed by the American colonists) have already found themselves a comfortable home on the benches of the federal judiciary. Since a few of the previously mentioned judges easily dismissed the particularity requirement of the Fourth Amendment's Warrant Clause, especially with regard to the roving intercepts of both wiretaps and bugs, then it seems to me that Judge Louie Brandeis' warning in his dissenting opinion of the 1928 *Olmstead v. United States* case has been validated once again, but this time it had nothing to do with national security or "terrorism" issues at all.

Fundamentally, I think the question at law to be answered is this – **are the contents of a cell phone equivalent to the "papers" enumerated in the Fourth Amendment?** Remember, the sequence of events matter; would anyone tolerate a Bluecoat rummaging through your drawers at home and seizing your papers *without* a warrant, simply because he testified on the witness stand later that he was concerned you might burn them before he arrived at your home? If not, then wouldn't flushing illicit narcotics down the toilet *before* a police raid fail to count as "destruction of evidence?"

Put another way, would wiping your cell phone *prior* to the issuance of a warrant be equivalent to burning your papers *before* the police are breaking down your door? If not, then why would it be considered "destruction of evidence" *prior* to the issuance of a warrant? Government prosecutors love it when statutory provisions are construed as broadly as possible by the judges for their witch-hunts, but absolutely hate it when defendants attempt to do the exact same thing in defense of their rights.

Truth be told, what these half dozen cases reveal is a profound lack of legal protections for cell phone users, regardless of the issues at law or the subject matter the facts of the case revolve around. The fact of the matter is that cell phone users are legally quite vulnerable to both data-mining and wiretapping by the police, and it should be clear by now that different types of Fourth Amendment challenges have already been tried and failed miserably. Unless someone litigates a test case by getting a federal judge to legally rule on determining what counts as Fourth Amendment "papers," then I don't foresee any other legal defenses against the federal judiciary using color of law to plant the seed for the fruit of the poisonous tree.

Digital Encryption's Trustworthy Security?

Believe it or not, the 1968 Wiretap Statute did not only authorize roving intercepts, but also the issuance of annual wiretap reports to the United States Congress. According to the 2012 Wiretap Report, total wiretaps were reported to be 3,395; in 2013, there were 3,576 total wiretaps, and 3,554 total wiretaps were reported for 2014. Interestingly enough, these latest three Wiretap Reports also had something to say about the increased use of encryption, respectively:

> *"Encryption was reported for 15 wiretaps in 2012 and for 7 wiretaps conducted during previous years. In four of these wiretaps, officials were unable to decipher the plain text of the messages. This is the first time that jurisdictions have reported that encryption prevented officials from obtaining the plain text of the communications since the AO [Administrative Office] began collecting encryption data in 2001."*
>
> *"The number of state wiretaps in which encryption was encountered increased from 15 in 2012 to 41 in 2013. In nine of these wiretaps, officials were unable to decipher the plain text of the messages. Encryption was also reported for 52 state wiretaps that were conducted during previous years, but reported to the AO for the first time in 2013. Officials were able to decipher the plain text in all 52 intercepts."*
>
> *"The number of state wiretaps in which encryption was encountered decreased from 41 in 2013 to 22 in 2014. In two of these wiretaps, officials were unable to decipher the plain text of the messages. Three federal wiretaps were reported as being encrypted in 2014, of which two could not be decrypted. Encryption was also reported for five federal wiretaps that were conducted during previous years, but reported to the AO for the first time in 2014. Officials were able to decipher the plain text of the communications in four of the five intercepts."*

Consider for a moment the implications of these findings. Although they admitted a specified number of encrypted wiretaps that they were unable to decipher, if you were to calculate the number of encrypted wiretaps they *were able* to decipher, I think you will find very quickly that they were able to decipher the **majority** of the encrypted wiretaps. If accurate, then that would mean that they can crack quite a bit of encryption, just not all of it, for some reason.

One likely reason this is the case, I speculate, is because different cell phone apps use different protocols. Shane Radliff engaged in consumer testing of various assorted cell phone digital encryption apps on his iPhone three months ago, yet while he seemed positive about his experience using those apps, he did point out that Surespot was mentioned in the *United States v. Ali Shukri Amin* case. According to the Statement of Facts, it says:

> *"On January 16, 2015, an overseas ISIL supporter communicated to the defendant via Surespot that the group of ISIL supporters, including RN, had successfully crossed over into Syria."*

Think about that for a moment – how would the prosecutor and defense counsel *both* **know** that a terrorist had

contacted Amin using Surespot? Unless someone snitched, the only other possibility I can fathom is that the call was intercepted by the National Security Agency and cracked; given the metadata would show that it was an overseas call, it's not unreasonable conjecture to say that the NSA hacked Surespot's encryption and discovered the nature of the communication between Amin and his associate.

What about the late FBI-Apple encryption dispute? It's been seldom reported in the mainstream media that FBI Director James Comey admitted that the Bureau paid over $1,300,000 to grey hat hackers to crack the San Bernandino shooter's iPhone. Once that was done, the (in)Justice Department withdrew its litigation against Apple that had attempted to coerce them into developing either a backdoor or a virus that would enable the Bureau to access the shooter's cell phone. According to Comey, the one-time hack only works on the iPhone 5C, but not the 6S or even 5S.

Does the FBI's outsourced hack of Apple's encryption really even matter? Back in 2009, Apple persecuted its own users for jailbreaking their own iPhones, because they alleged that doing so infringed on their copyright; it wasn't until 2010 when the Librarian of Congress made the decision to allow exemptions to what was otherwise the prohibitions on the circumvention of copyright protection systems (like digital rights management). Given that Ed Snowden whistle-blew Apple's involvement with PRISM only three years ago, I doubt Apple really gives a damn about users' privacy, which is why Mac users like myself have been gradually using more free and open-source software while lessening dependency on their proprietary software.

WTHR, an Indianapolis NBC affiliate, reported in 2008 about the prevalence of cell phone spyware, which had the capability to wiretap calls and geolocate the phone itself. Eight months later in 2009, WTHR's followup report featured a digital security firm that pioneered the capability to remotely backup and then wipe a cell phone using GPS tracking. This company's chief technology officer also said that they had developed software capable of detecting and removing spyware and viruses.

Although that might be comforting and rather forward thinking of them at the time, an Israeli firm known as Cellebrite developed technology exclusively for the "law" enforcement Bluecoats. Specifically, their UFED devices are used to perform computer forensics on cell phones, such as memory dumps, cross-referenced data analysis, and most alarmingly, defeating both user locks and encryption protocols. As one of Cellebrite's company pamphlets brags:

> *"As the sheer number of mobile numbers grows, so too does the volume and complexity of data they contain. Having the right mobile forensic tools at the ready to extract that data quickly has never been more important. The UFED Series delivers the most comprehensive mobile forensics extraction and decoding capabilities on the market. Flexible and secure, our unique solution makes it easy for forensic specialists to access and import mobile, location, private cloud and operator data from the widest range of mobile and GPS devices. With it,* ***officers, investigators and lab examiners can quickly and effectively bypass device user locks, decrypt encrypted data from rapidly changing device operating systems and recover texts, deleted emails, location information and account profile data*** *– and take appropriate action." [emphasis added]*

If a police officer like the one in the 2012 *Flores-Lopez* case had a UFED device, then the sky would've been the limit as to what other potential charges the prosecutor could have alleged. However, if UFED's data extraction technology has been around for several years, then it begs the question as to why the FBI didn't use their technology during the public relations controversy with Apple? Perhaps it had something to do with Fox News correspondent Carl Cameron's four-part exposé on Israeli espionage within the United States from back in

December of 2001. Cameron's reports showed that the Mossad had penetrated high-security federal buildings and made off with top secret documents; I don't think my conjecture that the FBI was suspicious of Cellebrite's likely working relationship with the Mossad is too far off the mark.

Unfortunately for most free software advocates, the typical mode of discovering the inefficacy of some digital encryption technology is by reading court documents. Although the judicial transparency is certainly good, this is a reactive approach, and even then, it only highlights failures. Might it be time to explore other approaches in learning about the efficacy of digital encryption that is more proactive in revealing *both* the successes and failures of such ventures?

An Economic View of Cell Phone Ownership & Usage

Why have cell phones become so popular in the first place? It could be said that the lack of commercial regulations against the burgeoning telecommunications industry might explain the unbridled success of cellular service providers, but this would seem to contradict the oligopoly of Big Telecom. Generally speaking, cartels do not favor the spontaneous order of the free market with their fascist business models, so how is it conceivable that market discipline functioned so well here with the development and marketing of cell phones amongst the general public?

Much like how inmates are able to smuggle illicit narcotics into government prisons, central planning can only go so far before it begins to buckle and crack under the weight of reality. Given that knowledge is dispersed, the slightest deregulation of otherwise quite onerous business regulations serves to reinvigorate the entrepreneurial spirit, and when coupled with the price system, this is the impetus needed for entrepreneurs to increase quality while lowering costs. Put another way, if the market is successful as it is under the most horrendous and trying of circumstances, then how much more effective would it be if those handicaps were absent?

A man's use value for cellular telephony increases the more his very livelihood depends upon it, regardless of whether digital encryption is available or not, whether user-friendly or not. The development of the cordless phone, followed soon after by the hefty car phone, demonstrated a growing market demand for mobility in telephony. Once the car phones became mobile enough to be battery-operated, then it was only a matter of time until they were capable of being handheld, and thus the cell phone was born.

Texting, picture messaging, and even videography (especially when coupled with Internet access), came not too long after cell phones had proven their use value across wide demographic varieties of people. It could be said that now the entire American population can be categorized in terms of their cell phone ownership and usage:

- Those who can live their lives fairly comfortably without any cellular usage at all, for it would mainly be a novelty for them since many of these folks lived most of their lives using landline phones, although it would also be fair to say that a contingent of these non-cellular users would be composed of neo-Luddites who refuse to use cell phones on principle.
- Others for whom using cellular telephony is a way to increase their social status and connectivity with friends and family; these would be the hobbyists and dilettantes who derive pure pleasure from calling, texting, and filming using their cell phones, even though their own use value for them is strictly recreational.
- A larger noticeable portion of the population began using cell phones as a way of maintaining emergency communications, as well as a way for both providers and dependents within family units to keep in close touch with each other regarding the daily routine business of life. A latchkey child's first exposure to cell phone usage typically begins against this backdrop, given that their parents have few other options available to them that can serve to keep tabs on their children from afar.
- The supermajority of cell phone ownership is directly tied to a person's reliance upon them as the facilitator of his very own livelihood. Whether it be an employer provided phone, or one that comes out of his own pocket,

> cell phone usage became ubiquitous because it enabled greater mobility in earning a paycheck. Fewer corporate staff meetings, fewer memos, and fewer progress reports to one's employer all resulted from the greater availability of an employee through his cell phone. Although this was probably the singularly greatest boom to worker productivity, the cost of it entailed keeping this relatively new device on one's person throughout the entire workday.

Granted, this is merely a sketch of how cell phone users could be conceptualized, it is simply a model for how to think about the purposeful behavior regarding the motivations driving cell phone ownership.

In passing, Uber ought to be mentioned here. This company's smartphone app has single-handedly begun real market competition against the licensed taxi monopolies strewn across America. As much as many would love the taxi monopolies to go embarrassingly bankrupt, it should be understood that Uber is, first and foremost, a ride-sharing smartphone app; obviously, this necessitates the use of a cell phone. Skeptics doubt that Uber would facilitate any form of end-to-end encryption for both drivers and customers, but at the same time, it would be most unwise to make the perfect the enemy of the good. Emergent technologies are usually built on top of preexisting ones, yet not everyone in the ride-sharing industry cares about individual privacy; so, as long as Uber remains plausibly legal, then privacy is a moot point, although it is foreseeable that a market demand in user-friendly encryption could arise should ride-sharing become outlawed.

A proactive solution that could be used to incentivize the development of not just encryption-friendly smartphone apps, but also in conducting security audits of free software, would be to organize various moneybombs. Tom Berson of Anagram Laboratories performed a security evaluation of Skype back in 2005 when he was given access to their proprietary source code; to be sure, Ed Snowden had some very choice things to say about this VoIP & IM service provider (specifically, that Skype became a PRISM collaborator on February 6th of 2011). Crowdfunding security audits is, I think, the best way to objectively determine any vulnerabilities in free and open-source software. Financial transparency ought to be provided by the fund managers, and the hired computer programmers who examine the source code can be held accountable when they publish a white paper detailing their results, thereby enabling the release of the funds they would have then earned.

The Medical Effects of Cell Phone Usage

A meta-analysis of the currently available scientific literature revealed that there are physiological effects from the microwave radiation (MWR) emanating from smartphones. The Journal of Microscopy and Ultrasound published a study in 2014, which suggested that children are noticeably more affected by MWR than adults are, simply because of their thinner skills, relatively smaller body sizes, and more absorbent brain tissues. Although the Morgan, Kesari, & Davis meta-analytic study included other devices such as laptops, I will confine my remarks here strictly to cell phones (Bluetooth devices were not mentioned at all in these studies).

One case study showed that tumors developed in spots on teenage girls' breasts where the cell phones were sewed into their bras. Another study reported a significant risk of brain cancer in regular cell phone use by children whose median age in the study was 13 years old; a similar Swedish study largely corroborated with the significant risk of brain cancer, but also with cordless phone use. Oddly enough, a study examining cell phone use amongst *adult* men showed that cell phone usage decreased "the semen quality in men by decreasing the sperm count, motility, viability, and normal morphology." Two corroborating Japanese and Australian studies revealed that lower sperm count, decreased motility, and DNA fragmentation were all resulting from cellular MWR; the Australian scientists in particular said:

> *"These findings have clear implications for the safety of extensive mobile phone use by males of reproductive age, potentially affecting both their fertility and the health and well-being of their offspring."*

Another scientist, professor Stanton Glantz at the University of California's San Francisco Medical School, concluded his own meta-analysis by saying:

> *"Taking all the information we have discussed on cell phones and sperm allows us to confidently conclude that exposure to cell phones adversely effects sperm."*

Obviously, the meta-analysis by Morgan, Kesari, & Davis wasn't limited exclusively to children, but don't necessarily think confirmation bias is at play here. The conclusion of their meta-analysis is that the risk to children and even adolescents from exposure to MWR devices is considerable, but also that adults have a very real risk, albeit a smaller one.

It is hard to argue that these studies are inconsequential, simply because they appear inconvenient to the bottom line of Big Telecom. If, indeed, the health risks are provably real and not just statistically significant, then consumers need to know that in order to make a truly informed decision as to whether the risks outweigh the benefits in choosing to own and use a cell phone. As can be expected, if your livelihood is utterly dependent upon using such an invention, then the question of whether or not such a device might put you in the midst of an electromagnetic soup seems more like an afterthought, because how else are you going to be able to pay the bills if you don't use a cell phone?

Socio-Cultural Adaptation of Cell Phone Usage

Pew Research Center has studied the practical realities of ubiquitous cell phone ownership for years. Generally speaking, all other forms of computer technology ownership falls behind that of cell phones , even laptop and desktop computers; also, the younger one's generation is, the more likely he is to own digital electronics. Generation X and Millennials have cellular telephone ownership in the 90th percentile, at 92% & 95%, respectively.

Interestingly enough, cell phones have been reported to alleviate boredom as well as a mechanism by which to avoid interacting with nearby people, and this is especially pronounced amongst Millennials. Assuming there is overlap of this with the purported rudeness of cell phone users while on a call , then the spontaneous ordering of cultural norms, as determined through individual market preferences, is going to be one hell of an adventure, to say the least. As a side note, I am rather dubious as to the spread of the generational gap, since Baby Boomers, Gen X-ers, and the Millennials are all pretty socialistic, for the most part; so, whatever cultural norms may emerge, it'll probably be based on some false notion of egalitarianism as advocated by the "social justice" equality freaks.

On a somewhat more humorous note, a study conducted by Ohio State University discovered that " distracted walking" was largely correlated to pedestrians who were so glued to their cell phones that they were struck by cars while walking in the middle of the road or literally walking off bridges into ditches. Calling someone was noticeably more distracting than just texting, they also found. While this might sound rather harsh, I think these idiots deserve

all of it; think about it, if you are so “busy” that you are not paying attention to where you are *walking*, then, frankly, you deserve whatever happens to you, truth be told.

Conclusion: Options, Solutions, & the Future of Telephonic Privacy

In light of the legal, technological, economic, medical, and socio-cultural realities that cellular telephony has brought to the table, then my original question about whether cell phones are mostly beneficial or noticeably detrimental to individual liberty must now be addressed. As I said earlier in the introduction, weighing both the pros and cons of cell phone ownership necessarily entails a thorough grounding as to how such an invention has a multi-faceted significance within your own life. Security culture is only valuable to the extent that its practitioners are less vulnerable to coercion than those who fail to take their right to privacy seriously.

It must be kept in mind that **cell phone ownership is voluntary**. There is no law that individually mandates that you *must* purchase a service plan, or else you go to jail and/or face a penalty or a fine. This is *not* an insignificant detail, for it sets the stage as to what my suggestions are for dealing with this invention.

First and foremost, you could take the Luddite route. Although it would make your life arguably more inconvenient, landline and even cordless phones still exist, so any utility you demand for telephony in general can be satisfied this way, and an additional plus is that there are far greater legal protections for those types of phones; besides that, they are noticeably less intrusive against your privacy, even if the content of your calls were being specifically wiretapped by the FBI (as opposed to being indiscriminatly wiretapped by the NSA).

Should you decide to use a cell phone for whatever set of reasons, then for goodness sakes, at the bare minimum, **USE ENCRYPTION**. Given the growing popularity of free software, their user-friendliness has greatly increased in recent years, so age-old excuses for not using digital encryption are going away, whether you like it or not. The most important forms of digital encryption I recommend you seriously consider are OTR for instant (text) messaging and ZRTP for your calls; an easy to use catalog of program applications can be found on the PRISM-Break website. More detailed how-to information for not only configuring these and other encryption programs onto your smartphone, but also for guidance about good information security practices while using your cell phone, are available via the Electronic Frontier Foundation’s Surveillance Self-Defense project, the Tactical Technology Collective’s Security-in-a-Box project, and the Privacy Rights Clearinghouse’s Fact Sheets.

A related pair of solutions involve both Silent Circle’s Blackphone and the Dark Android Project. I’m rather skeptical of Blackphone, not because I doubt Phil Zimmermann’s involvement in providing good security at all, but rather that their business model seems awfully similar to the Germanic Cryptophone. If you want no fuss secure communications, then expect to pay through the nose for it to the tune of at least several hundred dollars, never mind the ongoing maintenance costs of whatever service plan you end up using. By contrast, the Dark Android Project is more in the spirit of what the Free Software Foundation promotes; what the project’s mission essentially is are attempts to construct a cell phone, either literally from scratch or from a standard Android operating system, and then configuring its apps in such a manner as to provide the maximum degree of individual privacy possible using today’s available digital encryption technology, and at a fairly nominal cost, too.

Another related pair of mitigating options are those mentioned by the “odd couple” of a police detective and a satirical alternative media vlogger. Detective Cindy Murphy’s white paper on data extraction mentioned that:

> *“Isolation of a cellular phone in the field can be accomplished through the use of Faraday bags or radio frequency shielding cloths which are specifically designed for this purpose. Other available items such as arson cans or several layers of tinfoil may also be used to isolate some cellular phones.*

> *One problem with these isolation methods however is that once they're employed, it is difficult or impossible to work with the phone as you can't see through them or work with the phone's keypad through them. Faraday tents, rooms, and enclosures exist, but are cost prohibitive."*

Similarly, Montagraph's vlogs on improvised Faraday cages are a direct application of what detective Murphy was explaining. Needless to say, there is also the approach of simply removing the cell phone's battery whenever you're not making calls, but disassembling your phone more than once a day becomes a rather major pain after awhile, so perhaps Montagraph's approach of cost-effectively shielding your phone without disassembling the damn thing every time might be the best of all worlds here.

Ultimately, when it comes to the invention of the cellular telephone, you are going to have to make decisions involving tradeoffs between functionality and surveillance, whether the former of the two takes the form of text messaging, ride-sharing, or even using something that is still rather novel like crypto-currencies. Such decisions should not be made lightly, for your practice of security culture, or lack of it, will largely determine rather serious consequences for your freedom.

As for me, I personally regard cell phones as a tool I begrudgingly use as infrequently as possible, even to the extent of trading favors with others so I can borrow their phone in order to deliberately fail to maintain a reachable phone number, but that's just what I've been doing as of late. Perhaps over the years I'll morph into a real cellular tech-dweeb who can easily convert any Android phone into a nearly untraceable communications device that will become unparalleled in human history. As Cody Wilson once so beautifully phrased it:

LET THERE BE DARK!