Why I am against owning Cell Phones

(or: Why Replicant and other ROMs just aren't enough)

29 January 2016

Last updated: 05 March 2017

(See also, Why I am against iThings)

The Cell Phone and Smart Phone (though I call them DumbPhones as they are repressed computers that are counter-productive to the progress that computers have made in the past five decades) is something that now has become a part of our daily lives. This, I say, is for the worse.

It was recommended by software professionals (such as members of FSF) to have an alternative freedom-respecting ROM such as Replicant (the most freedom-respecting one). They say it would be the simplest way to use a phone while remaining a member of the GNU/Life. I know for a fact that this is another compromise to get others to join them, which I view as a con-outweighing-the-pro situation, and something they should stop doing.

I do not argue that using Replicant or another ROM is superior to using Android. It is increasingly becoming apparent, as with the new revelation that non-free software on almost all American Android cellphones were tracking the user and uploading their SMS data to China, with software implemented by the Manufacturer (not the American Company). My thought is that the software is not the issue here.

You see, free software is only one part of the problem. The entire way the basic cell networks work is harming privacy. I could give you reasons about **all** networks, including 0-Generation (Radio Telephones) through 2-Generation (Digital AMPS) but there would be no point as no provider even covers these anymore. In this Article, I cover the problems with the Modern Cellular Networks (3-Generation and 4-Generation) known as GMS and LTE.

- ### 1) E-911 (Enhanced 911) Services

  Enhanced 911 is a service legally required by the FTC to be implemented by every cell network in North America, including Canada and Mexico through collaboration with their Federal governments.

  How this works is simple. All cell phones connect to the Cell Tower. The Cell Tower is required to ping the telephone every 30 seconds. Using the time it takes to ping the telephone, the geographical location of the tower, and the rate of change in the ping, you can then locate the approximate location of the device, therefore the user. This can not be lawfully disabled, nor does it require GPS, though modern systems use it only as a factor in pinpointing the phone.

  This is for interest in public safety. The idea behind it is that if you were to call Emergency Services (which is 911 in America), the operator can find your location regardless of the fact you are mobile and out and about. Other countries have similar technologies.

- ### 2) Cell Phones can't tell Real Towers from Fake Towers

  You all know what a cell phone tower looks like, right? Well, to a Cell Phone, the tower looks like a data-transferring ping machine. Recent technological breakthroughs allow people to hijack cell phones knowing this. For example, a van that is traveling down the road can then enable a transmitter that simulates a cell tower (back-up link). This can be used by the modern pheaker to not only log your calls, invade your privacy, etc, but it can also be used to make phone calls using your own number.

  This also is proven to have been used by the NSA in 2011. The NSA had a large number of these fake towers that the cell phones would switch over to thinking that it's a normal network tower. Through this, the NSA logged all communications from the user.

  Not only does the federal level government use these devices, but local police precincts have begun to use them as well in an illegal method that many precincts courts have agreed to be without warrant or probable cause. In mid 2015, *USA Today* (back-up link) reported its use in a simple theft case in the city of Baltimore. The article also says similar devices are being used in Los Angles and Miami. The article says that the local police districts hide these devices and often times do not disclose information related to the devices, causing many judges —and even lawyers from both sides of the hearing — to not even know of their existence. This is morally wrong, a violation of the United States Constitution, a mockery of the American judicial system, and a great overstep in the jurisdiction of local police precincts.

  This technology has other purposes outside of law enforcement that are equally abysmal. **Advertising companies** *can and do* use it to track users in a technically-legal method, as *The New York Times* (back-up

link) recently reported, in a combination with surveillance cameras. This technology uses the fake tower technology to know who passes by it, who looks at it, and etc. Activist groups are already protesting against this should-be-illegal surveillance.

- **3) Using both technologies together can (and has proven to) strengthen spying**

  Using both technologies as above, the US Government used small aircraft to spy on the cell phone devices of the Black Lives Matters protesters in late 2015, as reported by *The Washington Post* (back-up link). The *post* reports that the aircraft was not only equipped with fake towers, but it also used the E-911 pinging system to track the locations of the owners without GPS ever playing a factor. An artistic vitalization of this is available here (jpg, twitter-hosted, 60 Kib).

These are ways that the GSM (or newer) networks can harm you. Although these are my primary reasons against this, there are more.

- **Even with a new ROM, virus attacks are possible (and more dangerous)**

  Just because you flashed a new ROM doesn't mean you are not vulnerable to exploits in the system, including viruses, malware, bugs, etc. Using a custom ROM helps this a lot, of course, but all things can be exploited, and nothing is 100% fool-proof. For example, all cell phones, even those running Replicant, can be turned into listening devices. Even if there was a way to disable the internal microphone. Using a simple software switch received through a virus, you could change the speakerphone speaker to be input instead of output.

  Although the software I speak of has not yet been developed, it is well within the realm of possibility of existing. Using the software is a very simplistic method of intrusion. Any speaker can be used to input audio instead of output it, really. A lot of people don't know this. I'll let you see this for yourself. Take your headphones, plug them into a mic port, put both speakers to your mouth, open a recording program, and yell. Congratulations, you have a low-quality microphone.

  Knowing this, the device doesn't necessarily need to transmit at all to send out your data. A virus could infect the phone, change the output into input using specially designed software, and set it to record to a hidden file. Eventually, when the user connects to wi-fi, it simply uploads it to a server through plain-old HTTP without the user knowing. This automatically makes it more dangerous than a regular computer, or a real phone.

  Virus attacks can also lead to everything a virus or malicious program can do on an actual computer. Also, just because Android uses the Linux Kernel, that doesn't mean it can't get more viruses than a normal GNU/Linux system. There are many viruses that affect Android **directly**. These viruses can also affect Replicant. You can get spyware, malware, etc. If you get a spyware device on your phone, and knowing it had location services that you can't turn off (literally), you are then a victim of a whole new, unexplored territory of Cyber-Crime.

- **Dumbphones can be made into listening devices WITHOUT a malicious software switch**

  Some DumbPhones have a special circuit, where the cell modem is connected to an Analog to Digital Converter. This A2D converts analog input to the speaker, digitize it, and then saves it into files that can be uploaded at a later date. This allows the DumbPhone speaker to be converted to a Microphone without a specialty software switch like I said above. The recorded sound can also be broadcast on the phone to a nearby reciever through radio transmission, but these types of systems only work if you are being targeted. The upload via the internet can be done by anyone, including myself.

  Think of this: A large majority of phones actually have a **backdoor built in their modems**, allowing others to access them not only for sound, but for other malicious purposes, *with no effort*!

- **DumbPhones are contradictory to the progress of computing**

  This reason is purely philosophical and a point of personal preference. *You can choose to ignore this one.* This is in no way malicious, however you could view it as a form of Hardware DRM.

  The progress of the computer led to the desktop and then the laptop for portability. The IBM-Compatible (now called "Wintel" by many) system became the dominate on the market. This is a good thing. With IBM-Compatible systems becoming a computer standard, everything can be compatible with everything. Technically every modern computer (except Apple) is a clone of IBM, thus IBM-Compatible. This is not a monopoly because other companies were simply using the IBM system to make their own systems, IBM receiving no royalties. Atari and Commodore couldn't provide that, thus IBM clones became commonplace.

  However, the modern tablet and DumbPhone (both designed for convenience) are contradictory to this. Without standardization, they are computers that therefore fight the pursuit of progress. Dumbphones are watered-down computers that can not be compatible with any other system directly. What is truly sad and downright appalling is that they are predicted to replace the Desktop and laptop computer. All the

DumbPhone is: A PDA bundled with a Cell Phone. Q.E.D.

You can read more about this issue in three places: *Where did the Computer Go?* by Dragan Espenschied, *Turing Complete User* by Olia Lialina, and *What Made the PC, Mac, and Linux so Great (or not)* by Nathan "Toasty Tech" Lineback. An article worth reading that is not quite on this topic but touches similar philosophical areas is *Rich User Experience, UX and Desktopization of War* by Olia Lialina.

What do I do?

I carry 50 cents when going outside just in case I need to make a phone call. Pay Phones still exist despite what the general population and media might lead you to believe. Furthermore, simply asking the local business to make a quick phone call usually works. I have no reason to ever make a phone call when outside, except maybe when I travel. That is also a rarity. Still, it is good for a just-in-case.

If I have an urgent call I am expecting, I stay at home and wait for it to be answered. If it is somewhat urgent, I go out and check my answering machine when I return.

Some things to consider:

Think of this: Do you really have someone that you need to call so urgently that you need to carry a communications device on you at all times? As I said before, I just use my answering machine.

If you use a DumbPhone for listening to music in your car, just switch to the radio or play a CD. It's not too bad. Sometimes the audio quality is even better.

If you use your DumbPhone to mindlessly search for funny photos of things, then you are dumb. That in and of itself is a normie thing to do, and you should stop it as soon as possible, but you can simply wait to use your computer at home if you must.

Texting is obsolete in and of itself. Of cell phone users I have seen, most don't use actual text, but instead use other methods such as the Kik "app". If you can use an "app", you can wait to use IM software on your computer at home.

Using a cell phone in a home itself is a stupid thing to do. Having the phone company give you a land-line (and perhaps an internet connection if it is Freedom-Friendly™) is superior to using a small device that goes out if there is a lightning storm outside. Land-lines are wires. Cell Phones are wireless. Using a wireless anything within your home is odd, for a number of reasons. Also, a home phone goes for $20 a month. The average modern cell-phone plan is around $80 (with data, which is something that most services force the user to pay for regardless.) That is a singular reason to change right there.

Conclusion

In conclusion, changing the ROM to a freedom-friendly ROM on a DumbPhone is not enough. Also, if you are a Doctor, a Taxi-driver, a contractor, or something else that requires you to have a cell-phone on you at all times, you *may* need a cell phone. Otherwise, stop it. You really aren't that important. I think that a pager would be a better choice as it has less chance of monitoring due to them simply receiving text and phone numbers that you respond to later on another device.

©2016 Se7en
CC0 Universal/Public Domain

To the extent applicable by law, Se7en releases this article to the Public Domain under the agreement of the Creative Commons Zero license. This work was published in the United States.