Hello, and greetings from the Central Office! This summer has brought surprisingly little travel to far-flung corners of the world. My employer has kept me in a management role, but I’m now working on a lot of mobile technologies. This is really where the action is. Very capable smartphones are selling for as little as $50 nowadays, and the rate of POTS disconnections and port-outs is only accelerating. However, the company is actually holding its own in broadband. This is being done through deployment of fiber-to-the-node, a topic for a future column. Broadband, however, is an unregulated service, like wireless. The days of PUC-regulated POTS lines, however, are clearly numbered. In the past year, things have changed very rapidly - from consumer expectations about reliability to the plummeting price of wireless voice service (which, as of this writing, is actually free from ringplus.net, a Sprint MVNO) to the way that people purchase handsets, choose carriers, and pay for service (contracts have been all but eliminated thanks to T-Mobile’s competitive moves).

And then there’s the inside of prisons. Remember the kid a few years ago who was dealing drugs from the payphone outside the Central Office? He called me the other day from prison. From his cell phone. And he made it quite clear that he wasn’t pleased with my “service monitoring” that led to his current residential arrangement. I was a little taken aback, but not surprised. While federal prisons have somewhat kept pace with the evolution of technology by allowing prisoners access to limited e-mail technology, no prisons outright allow unfettered access to wireless phones. This hasn’t stopped the proliferation of them inside prisons, though. It’s actually a huge problem because a smartphone in the hands of an imprisoned and violent gang leader, for example, could be easily used to continue running a criminal organization from “inside.” Or to harass me, for that matter. More commonly, though, prisoners use mobile phones to keep in touch with friends and family, and they have no criminal intent. They simply cannot afford to pay the extremely high prices charged by Global Tel*Link and other prison phone providers. And there is a matter of both safety and convenience; prisons seldom provide enough phones for inmate use and there is often violent confrontation over access to the few phones available.

Cell phones are also a lucrative source of income for corrupt prison guards, who are paid relatively low salaries. A simple TracFone can command up to $300 in prison. This is as equally profitable a revenue stream for guards as drugs are, but with less risk. Guards caught smuggling cell phones might lose their job, but are not subject to prosecution for a drug felony. Additionally, the demand in prison is higher than for drugs, and the safety risk to guards by an inmate with a mobile phone is perceived to be less than that of an inmate high on drugs (or, even more dangerously, alcohol). What’s more, phones are periodically confiscated, often by the very same guard who sold them to a prisoner! This leads to a perpetual income stream. Sometimes seized contraband phones are even resold to other prisoners. In my view, it’s somewhat ironic that corrupt guards have become the primary competitor for the corrupt kickbacks paid to the prison system itself by operators such as Global Tel*Link.

Guards are the primary source of mobile phones in prisons, but they’re sometimes smuggled in via other means. One prison in Russia discovered a cat that was wearing a vest with pockets full of mobile phones. It was enticed by prisoners to slip through the fence in exchange for food. Another prison had to install nets above its prison yard because of a number of incidents in which mobile phones were delivered by drone. In France, a truck was discovered with a false bottom and, rather than weapons or drugs, the contraband was - yep, you guessed it - mobile phones.

Smuggled mobile phones have been a serious problem for prison authorities for some time. In 2007, An Omar Broadway Film was clandestinely shot in the Northern State Prison in New Jersey. Contraband phones are prominently featured. Prisoners using mobile phones is such a common problem that Facebook even has a procedure for prison authorities to request the removal of Facebook accounts corresponding to users who are in prison (Facebook doesn’t allow prisoners to use the service). It’s also common to find videos on YouTube shot from prison; they show everything from the mundane details of everyday prison life to rap battles. And obviously, this is just the tip of the iceberg. It doesn’t take the intelligence level of a hacker to know that you should probably keep a low online profile if you’re in possession of a contraband mobile phone. So now, we’re starting to see some high-tech and low-tech solutions to combat the problem.

In many countries, there is a fairly blunt instrument that is employed to combat the issue: jammers. Wardens in the U.S. have pushed the FCC for years to allow this in prisons as well, but the FCC unequivocally bans jammers in nearly all circumstances (the Secret Service reportedly has an exemption from this
ban for purposes of protecting the President’s motorcade). The CTIA, a lobbying group for mobile phone companies, strongly supports the ban and opposes all use of jammers. This is, in my view, the right call; it’s not reasonable for neighbors of a prison to be impacted by measures intended to prevent prison contraband. After all, a prison’s neighbors aren’t actually in prison themselves! So wardens have mostly resorted to low-tech measures: searches.

It is possible to train dogs to find mobile phones, and some prisons have done so. However, dogs are trained to smell electronics, not mobile phones, and a lot of electronics are actually allowed in prison. To a dog’s nose, portable music players are nearly indistinguishable from mobile phones, and almost every inmate has a portable music player. So, dogs are really only effective at a prison’s perimeter. They can help to find a stash of mobile phones secreted away in a hidden vehicle compartment, but they’re all but useless inside a prison.

Prisons can also - in theory - hunt down unauthorized mobile phones using RF gear. After all, mobile phones broadcast within narrowly defined frequency ranges so, at least in theory, it should be possible to detect them. In fact, it’s considerably more difficult. Prisons are made out of concrete and steel. This means radio signals reflect all over the place. Inmates live in very close quarters, and a very large number of them have mobile phones, creating a fairly massive amount of activity. What’s more, there are a lot of authorized mobile devices inside prisons. Guards in many facilities, for example, are allowed to use their personal mobile phones in designated areas. Some prison doctors are allowed to use portable hotspots or personal mobile devices to look up medical information. The list goes on. Prisons using RF gear to find mobile phones have almost the same results as prisons conducting random searches.

In California, however, the state prison system may have discovered a method that works. In partnership with a mobile carrier (such as my employer), a special cell tower is installed within the prison walls. It essentially functions as a repeater that filters by IMEI or ESN. Here’s how it works: authorized devices (along with the devices of claiming neighbors) are added to a whitelist. Every other device is blocked from accessing the mobile network, and an intercept message is played explaining how authorized users (e.g. people not in prison) can resolve the situation. Text messages and data services are also blocked. Such systems are blandly called “managed access solutions” and operate very similarly to Stingray devices used by law enforcement. However, these devices actively interfere with traffic rather than passively monitoring it. Sound good so far? There is a dark side. The largest provider of “managed access solutions” is a company called Securus, which provides inmate calling services at inflated prices (with requisite kickbacks to prisons). Obviously, their motive for being in the business is to protect prison phone revenues. Another company, meshDETECT, also provides these devices. However, their systems are more pragmatic; they can be configured to allow inmates to use cell phones, but ensure that they are subject to the same monitoring (and naturally, billing) as any other call made from a prison phone.

It’s obvious that the current situation, where inmates have virtually unlimited access to mobile phones, is untenable. Most people don’t belong in prison, but some inmates actually do belong there and have committed serious violent crimes. These offenders in particular shouldn’t be allowed the relatively unfettered ability to continue directing criminal enterprises from behind bars. On the other hand, the vast majority of inmates with mobile phones just want to stay in touch with their family and significant others, and they don’t want to bankrupt these people doing so. They don’t actually present a threat. The technology exists to allow inmates access to mobile phones, but for this access to be monitored. As mentioned, it’s called Stingray, and this is a technology that is not only widely used in criminal investigations, but it’s already FCC approved. I think a reasonable compromise is to employ a Stingray inside all prisons, play a message indicating that all calls are monitored, and allow inmate handsets to be registered. However, mobile carriers should continue to provide the service at normal (not inflated) rates. Allowing greater access to (monitored) e-mail services hasn’t resulted in any significant problems in federal prisons, so expansion of (monitored) access to mobile phones shouldn’t result in significant problems either.

And with that, it’s time to bring this installment to a close.

References

http://prisoncellphones.com/ - Lots of information about meshDETECT, a managed access solution.
http://gcn.com/articles/2013/09/05/prison-cell-phones.aspx - Good roundup article of managed access solutions from GCN.
https://www.fcc.gov/document/contraband-wireless-device-nprm - FCC notice of proposed rulemaking for contraband cell phones. The essence of this is allowing managed access, but disallowing jammers within prison walls.
https://securustech.net/phone-services - Securus provides managed access solutions, but they appear to do this primarily to protect revenue from inflated prison calling rates.
https://www.youtube.com/watch?v=EBIt0rMBVqU - Video roundup of camera phone shots sent from inside prison. A good look at prison life.