Article development led by **acmqueue**
queue.acm.org

Stopping Big Brother would require an expensive overhaul of the entire system.

BY POUL-HENNING KAMP

Surveillance Too Cheap to Meter

DURING HIS KEYNOTE address, risk management specialist Dan Geer asked the 2014 Black Hat audience a question: “What if surveillance is too cheap to meter?”

As is the case with electricity from nuclear power, technology has little to do with it: This is a question about economy, specifically the economy of the path of least resistance.

Surveillance is ridiculously cheap for governments. Many have passed laws that obligate the surveillance industry—most notably, the mobile network operators—to share their take “at cost,” and we know law enforcement uses it a lot.

So why is so much cheap surveillance available for purchase?

Telephones work because telcos can route calls to and from them. The backbone and its routing tables are trivial compared with the airgap from the mobile base station to the wireless device, where there is no escape from knowing which phones are where.

Because bandwidth is limited and everybody and their Internet of Things (IoT) gadget has a SIM card these days, the density of mobile base stations has increased, which has reduced the uncertainty of the position from tens of kilometers in the 1960s to tens of meters today.

In theory, a mobile network company could throw away that information the moment the mobile phone moved to a different location—and they do anything but.

First, collecting data is deep in telco DNA. If you try to convince them not to, Mr. Prosser answers, “It’s a call data record! You’ve got to collect call data records!” If you really press the networks, they will tell you old tales of people refusing to pay for long-distance calls being taken to court and shown the evidence. Never mind that today, nearly all contracts are fixed price and people complain only when they get hit with predatory charges from third parties, cruise-ship networks, in-game purchases, among others.

Second, the data can help diagnose trouble in the network for the first few days. This was quite important in earlier generations of mobile networks, but not so much now.

Third, it is truly interesting data. AT&T used to send out press releases about how many holiday calls they had handled each year; similarly, modern telcos often boast how many handsets have been at sports events and stadium concerts.

But, most importantly, it is cheap data. It pours out of the system whether you want it to or not, and disk space costs nothing.

To stop the surveillance, the mobile networks would have to get their equipment suppliers to make changes; they would have to change their own back-office systems; they would have to reformulate customer contracts so they would not rely on the data being available in case of disputes; and so on.

Even ignoring the fact that lawmakers have generally made the collection of surveillance data a requirement for

IMAGE BY DA_ART/SHUTTERSTOCK

mobile network licenses, it would cost the telcos more money to stop the surveillance of their customers than to continue doing it.

That is quite literally what “surveillance too cheap to meter” means.

The fact that telcos have subsequently found other customers for their surveillance data—for example, customers presenting themselves as “market researchers” but often fronting for private or public intelligence agencies—only makes matters worse.

On the other side of the wireless connection, there are only two games in town: Either you are Apple, or you put Google’s Android smartphone soft-

ware on your product. Both platforms are architected on an economy of surveillance.

There is objectively no reason why Apple or Google should know every single time you make a phone call or send a message, but since their profits are built on them knowing, you will not find it easy to configure your mobile phone to *not* tell them—and you will be constantly pestered by ominous warnings and notifications if you manage to do so. My phone spends four to five seconds trying to tell Google about incoming calls, then raises a notification about its failure, resulting from my failure to configure

it correctly, and only then does it activate the ringtone.

If you write an app for either platform, you must publish it through the respective walled garden, and you can do so for free—but then it must contain built-in advertisements that provide Apple and Google with surveillance data of your users. If you want to protect your users from that, you must sell the app for money and hand over a cut to compensate Apple and Google for the missing advertisement and surveillance revenue. The platform itself will, of course, still report when, where, and how your app was used.

This again is surveillance too

cheap to meter: It literally costs money to reduce it, and in this case, you eliminate it entirely only by not having a smartphone.

Switching back across the airgap again, you would hear, in arguments proffered for rolling out a new generation of mobile networks, such verbiage as “better streaming,” “better gaming,” and “a generally better mobile experience.”

The last one is the truthful one, because all the surveillance nailed onto the content the user wants means that most mobile experiences are fairly lousy compared with what they could be.

It is almost always the case that more than a dozen—and often several hundred—organizations get to know which website you are trying to reach, and what you want to see on it, before you ever get to see any of it. It is simply part of an electronic auction to sell the advertisements you will shortly see.

How else could “targeted advertising” be implemented?

This takes an incredible amount of round-trip times (RTTs), which is why work on HTTP in the past 10 years has had a laser-like focus on avoiding TCP’s three-way handshake by any means imaginable, while at the same time trying to obscure—as much as possible—precisely how much and which surveillance data the big platforms are collecting.

If you do not believe this, try browsing the Web with JavaScript disabled. Yes, a lot of sites look cubistic or even impressionistic because their “reactive” design relies on JavaScript, but you will be surprised how fast generally sluggish websites suddenly become when freed from their heavy coat of surveillance gunk.

This is also why the latest generation of mobile networks has been designed with a very hard focus on RTT. As Claude Shannon, the father of information theory, showed that costs more bandwidth, which means higher carrier frequency, which means shorter reach, and, therefore, a much denser network of mobile base stations. Thus, the mobile network will triangulate your next mobile phone to within a few meters.

Customers will be paying for a brand-new mobile network to lower the cost of surveillance, further paving

Facebook uses DNS requests to spy on just about everybody on the Web by always forcing the lookups to go all the way back to the mothership.

the road for more of it, and they will not get a “generally better mobile experience” for their money.

Facebook delivered the perfect case study of this when it botched its Border Gateway Protocol (BGP) routing in early October and took its Domain Name System (DNS) servers off the Internet.

DNS was designed to avoid precisely that very problem, but Facebook uses DNS requests to spy on just about everybody on the Web by always forcing the lookups to go all the way back to the mothership. Whenever you see one of those “Share this on Facebook” icons on a Web page, your browser makes a DNS request and an HTTP request directly to Facebook’s servers to get that little image. No caching is allowed by the responses, and those requests feed directly into the maws of Facebook’s surveillance monster.

Because Facebook’s DNS responses are uncacheable, all the spyware it has distributed, desperately trying to tell Facebook what everybody was doing, hammered DNS-resolvers all over the network—precisely the opposite of what Paul Mockapetris intended with RFC1034.

So, yes, surveillance is too cheap to meter, and that just might be why Dan Geer now lives on a faraway farm with terrible mobile coverage.

IT nerds tend to find technological solutions for all sorts of problems—economic, political, sociological, and so on. Most of the time, these solutions don’t make the problems that much worse, but when a problem is of a purely economic nature, only solutions that affect the economics of the situation can possibly work. Neither cryptography nor smart programming will be able to move the needle even a little bit when the fundamental problem is that surveillance is too cheap to meter.

Either we slap a stiff tax on surveillance data, or we learn to love the panopticon.

Poul-Henning Kamp spent more than a decade as one of the primary developers of the FreeBSD operating system before creating the Varnish HTTP Cache software, which around a fifth of all Web traffic goes through at some point. He is an independent contractor; one of his most recent projects was a supercomputer cluster to stop the stars twinkling in the mirrors of ESO’s new ELT (extremely large telescope).

Copyright held by author.