WHAT?!?

AN UNPROTECTED SMARTPHONE?

WHY PEOPLE WHO KNOW (E.G., INTELLIGENCE AGENCIES)
DON'T LET PHONES INTO THEIR FACILITIES.

PRIVORO®

Be Aware

If you hold, share or have access to important enterprise, government or personal information, you should operate as if your smartphone has already been hacked.

THE RISK OF LEAVING SMARTPHONE SENSORS UNPROTECTED.

There are more than 20 "legitimate" companies around the globe creating and selling smartphone malware, not to mention the deep pool of sophisticated nation-state resources dedicated to the task. This malware gives attackers access to the highly sensitive microphones, high-definition cameras and location-tracking RF sensors that come as standard features on smartphones. And for those malicious actors not big enough to buy from these mega-players or for those who can't develop their own attacks, similar malware is available on the dark web for a nominal monthly fee. What about mobile security software? Well-publicized attacks at both the firmware and RF levels slip right by those protections. As reported in a 2018 summary of Spectre and Meltdown, chip-based attacks are inevitable, if not already creating havoc without the detection and remediation of this new exploit. Translation – few, if any, barriers will effectively keep hackers out of your phone if they think you have something of value.

CONSIDER THE RISK TO YOUR COMPANY.

A single conversation overheard from the microphones on your smartphone – whether at work, home or in the offices of customers or partners – might be all it takes for a competitor to gain a geo-political, strategic, marketing, product development and/or financial advantage. Intellectual property, M&A plans, research and development, earnings… pretty much everything that underpins the success and failure of a company starts with a discussion long before it is written down. And these conversations don't just happen between work colleagues.

I Tracked Myself With $170 Smartphone Spyware that Anyone Can Buy

"It wasn't some top-secret government program, or an expensive piece of surveillance gear that made this possible. It's something anyone can do for as little as $170, or sometimes less."

— *Motherboard*, February 22, 2017

> "Fundamentally, we're going out there stealing information we are not otherwise entitled to. Now, we do it to foreigners. … But unarguably, we're out there stealing other people's secrets."
>
> — Michael Hayden
> Fmr. Director of the NSA
> Fmr. Director of the CIA

Even with all the non-disclosure agreements and security clearances, people talk – especially to those they trust. To spouses, family and friends. And, the topics covered could compromise the entity for which they work.

CONSIDER THE BIGGER PICTURE.

Economic security underpins national security. Foreign powers are hungry for the unpublished and undocumented information they can get on enterprise businesses as well as on federal, state and local governments. Knowledge is power, information is digital and phones are the portal through which a great deal of data flows. Compromised smartphone sensors can capture pricing information, expansion plans, go-to-market strategies and more. Some nation-states share this type of information with businesses in their own country to make them more competitive. Don't believe it? Multiple countries have already owned up to it, including the United States, as stated by Michael Hayden, former director of both the NSA and CIA.

CONSIDER THE LIABILITY TO YOUR COUNTRY.

The U.S. government states that it doesn't share what it steals with private industry, but no other country has the luxury of being the world's largest economy. Most countries fight an uphill battle in which every advantage counts.

The threat is greatly amplified when executives and government officials do business on foreign soil, giving that country a home-field advantage. Understanding this, most sophisticated companies give their executives burner phones and laptops for overseas travel, even though that doesn't stop in-country meetings from being surveilled by the compromised phones that are present.

Be Aware

"Cybercrime constitutes the 'greatest transfer of wealth in history.'"

— Gen. Keith Alexander (Ret.)
Fmr. Head of US Cyber Command
Fmr. Director of the NSA

Bottom line: If you think you only need to worry about unsophisticated script kiddies, you're mistaken. Cyber warfare is asymmetric and companies, governments and high-value individuals face nation-state level attackers all day, every day. Every breach potentially strengthens one company or government at the expense of another. Cyber espionage is estimated to cost hundreds of billions of dollars per year, an amount that makes a difference to even the largest countries.

Don't think you need to protect your smartphone along with all your other electronic devices? Think again.

Smartphones are incredible tools, but the consequences of unprotected sensors falling under the control of malicious actors continues to alarm security experts.

Now is not the time to be afraid, but to commit to vigilance. The threat is real. New solutions exist. Learn how to protect yourself, your company and the people in your charge. Visit Privoro.com.

PRIVORO®