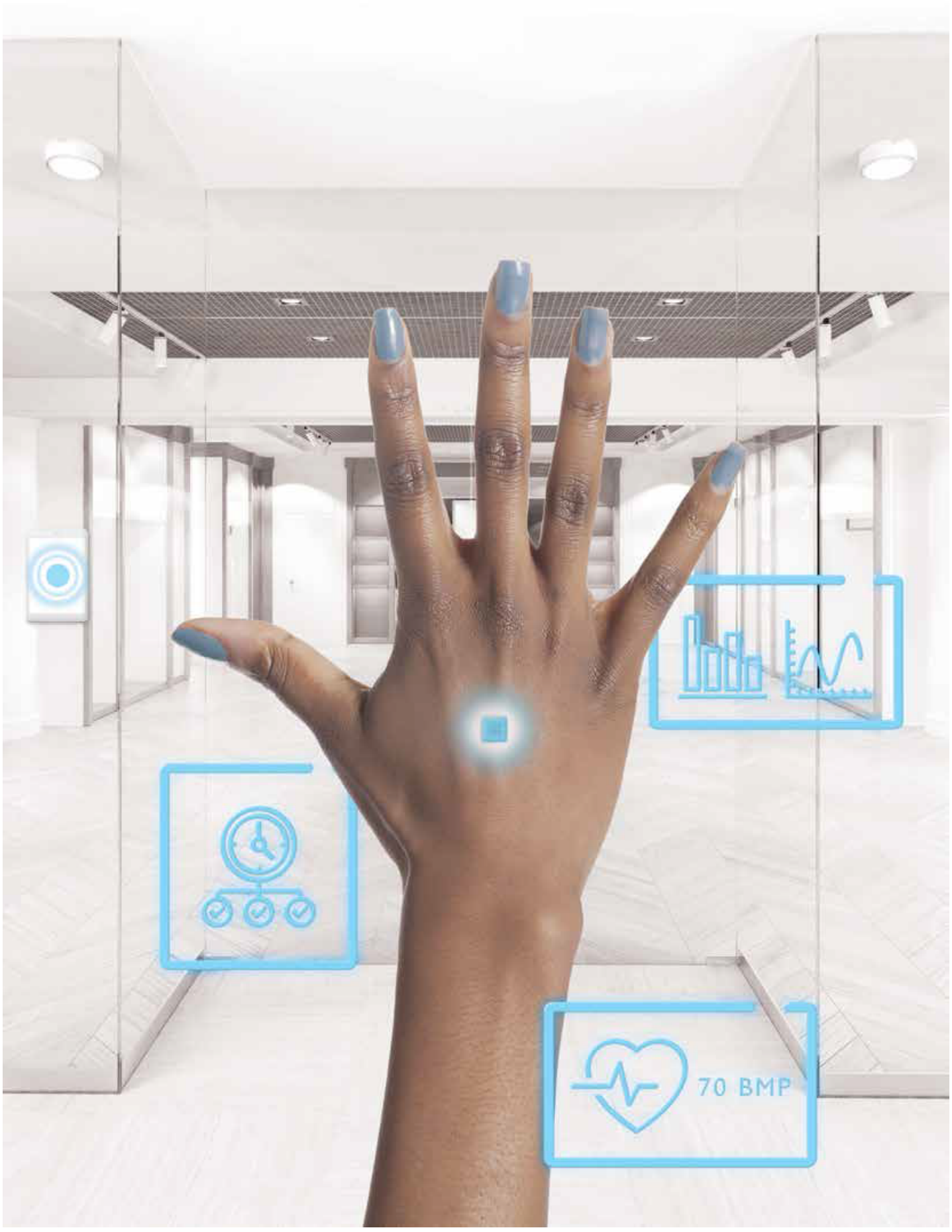
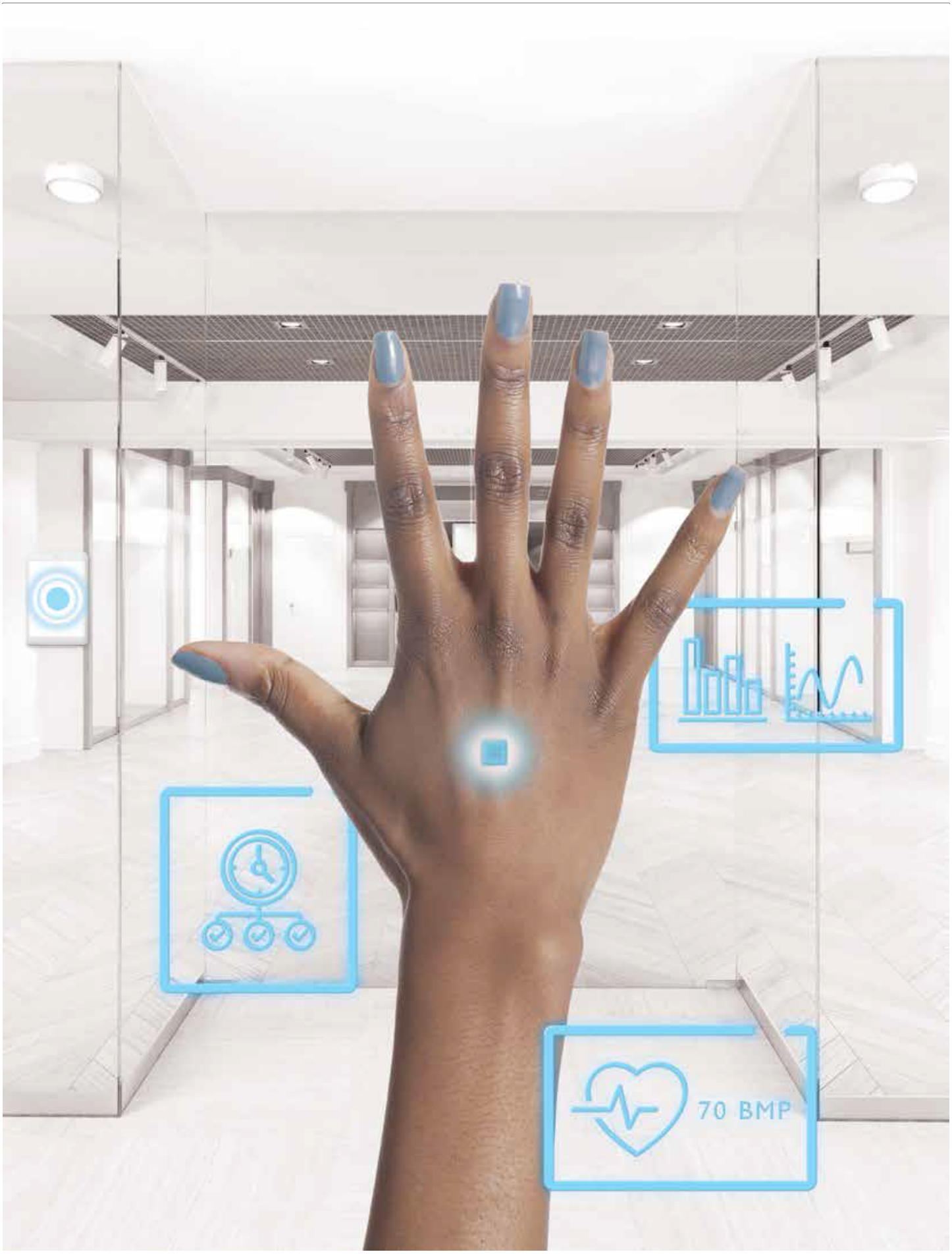
Invasion of the Body Hackers

Technology, Privacy, and eCommerce


70 BMP


70 BMP

CHEAT SHEET

- ***Not just wearable.*** Implantable devices raise more questions about privacy when they cannot be easily removed.
- ***Medical vulnerabilities.*** Body Area Networks, localized wireless networks that monitor health, can be manipulated by bad actors.
- ***Privacy by design.*** The concept anticipates all potential use and misuse of information. Consider not just what "can" be done but also what "should" be done.
- ***Data retention.*** Manufacturers need to consider how much data needs to be kept and what controls users will have to delete (or request deletion of) data or to otherwise set retention parameters.

Last Halloween, as I hastily prepared my Frankenstein's monster costume, my mind wandered to privacy. Why privacy? It all started because I was wondering what all those little bolts on Frankenstein's neck did. Sure, they helped conduct the electricity that brought the creature to life, but what if they actually did more than that? What if Dr. Frankenstein used those little implants to monitor all sorts of things about his monster? What if he wanted to monitor where the creature wandered to when it left the castle, what its peak heart rate was when it ran from those pesky villagers, and what happened to its pulse when it first laid eyes on its bride? Would this kind of control be a good thing? Would the "good" doctor have considered what information to collect and whether Frankenstein consented to sharing it?

I realize all of this is probably just late night random musings of a privacy professional on her favorite holiday, but these thoughts are no longer as monstrous as they once seemed. The merging of the devices we rely on and the body that we inhabit is no longer just scary bedtime reading.

I know what you did last summer

Not just wearable, but implantable, computing devices and sensors have been popping up in unexpected places this year. Last summer, there was anxiety when the company Three Square Market offered its employees a strange opportunity: The employees could implant a rice grain-sized chip in their hands to provide easy access to conveniences like making snack purchases, opening secure doors, and logging in to devices. Implanting the chip wasn't mandatory, Three Square Market reasoned, and employees could choose to use external devices for the same purposes. But the idea of a sensor becoming one with its host provided lots of interesting summertime cocktail conversations for privacy professionals. Some questions included:

- Would employers use these chips to monitor employee work schedule, compliance with policies, or time spent on breaks?
- Would the chip ever be truly "off " or would it keep tracking during personal time, allowing access to locations such as home address or the school addresses of children?
- Would employers share the data with other employers or third parties like insurers or other benefit providers?
- If payment card data or employee access credentials were stored, what security kept that

from being remotely accessed and stolen?
- If the employee spent too much time in the onsite healthcare center, would that be a sign of a chronic disease or illness that management would want to know about in terms of cost/payment/productivity?
- Where did the chip go if the employee quit or was fired? Could the employer force a second medical procedure to remove it or would it be remotely wiped?

The idea that an employee would make such an invasive commitment to sharing personal data in exchange for more easily using the vending machine was a stark reminder for privacy professionals: We need to continue to educate while also providing creative solutions to protect users without impeding the rollout of new technology. The convenience and immediate access that a new generation demands — and that technology is increasingly able to provide — is a tempting treat many are willing to readily accept, especially if they haven't thought through the potential tricks that may result.

The tell-tale heart

While novel in the employment context, implantable devices are not as new in the medical field. Body Area Networks (BANs) are highly localized wireless networks that are able to support a wide variety of medical applications such as monitoring the functioning of implants like pacemakers, tracking vital signs, or even performing internal exams. Sensor nodes are placed either in the body or under the skin and programmed to provide relevant data. Medical professionals using an external device can then access the information, whether it's a mobile phone or other enabled system. The benefits of this real time data source are significant. These sensors provide immediate access to the patient, wherever they may be located, enabling early detection of life-threatening issues. While the extent of this new age of medicine is hard to fathom, so too are the inherent risks. What was once make-believe is now rapidly becoming reality.

Fans of the Showtime series *Homeland* may remember the episode in second season "Broken Hearts" when one of the main characters, Brody (played by Damien Lewis), is forced to provide a terrorist with the serial number to the vice president's pacemaker to save the life of the protagonist, Carrie (played by Claire Danes). The terrorist leader assassinates the vice president by remotely manipulating his device, causing a heart attack. When the episode aired in 2012, the plot was dismissed as pure fantasy. It was later determined a credible threat and additional security measures were extended to protect then-US Vice President Joe Biden from a similar attack. BANs are vulnerable to a huge number of attacks and threats. For example, a bad actor can capture or incapacitate a sensor, sending false information to a physician or other individual relying on the data transmission. This could result in a hazardous life-threatening situation, failure to block a physical security threat, or the loss of an important trade secret. An adversary might also take advantage of techniques like jamming and tampering* related nodes or sensors to block an entire network or sending mass numbers of irrelevant packets to paralyze a system allowing additional time for a more surgical attack (i.e., while the metaphorical cameras are down, the jewelry thief walks right in the front door).

*Jamming and tampering are essentially attacks that effectively cause a denial of service or either transmission or reception functions.

Enter the cyborg

Not all implantable medical devices are as subtle as a tiny chip or invisible as a pacemaker, and accordingly the security and privacy questions they raise are different. Artist Neil Harbisson garnered a flurry of attention when he presented himself to the world as the first "cyborg." He sports, hanging conspicuously over his head, an implanted "electronic eye" that allows him to hear the colors that his eyes do not allow him to see. The antenna is a permanent device implanted into his brain that translates colors into sound frequencies so that Harbisson can see, for example, the color yellow by hearing the note G. Harbisson has expanded his capability from seeing only black and white to seeing hundreds of colors in varying shades and, in a TedTalk, described how he and technology have become one:

"I feel that I am technology. I don't feel that I'm wearing technology. And I don't feel that I'm using technology. I feel that I am technology. I feel like the antenna is a part of my body, which is an unusual feeling, but it makes sense. When you've been wearing it for so long, your body just accepts this as a part of you."

Other cyborg wannabes, referred to as "grinders," take implantable devices to the next level. In garage labs around the world, grinders embed their bodies with RFID tags and other devices that allow them to unlock doors, access their smartphones, turn lights off and on, or simply "to glow." Even entrepreneur Elon Musk has jumped on the bodyhack bandwagon, creating the new company Neuralink, which he pledges will produce technology to link human brains with computers using implantable chips within four years.

In some cases these devices are obvious while in others they are invisible. In each case, however, there is little way to truly monitor what kind of data is being collected and when the data is being sent and received. Could a novelty implanted RFID tag be secretly used by its host to hack into and skim credit card RFID chips? Could an antenna, like Harbisson's, be used to capture video of unsuspecting third parties or companies? Such uses may not be that far off.

Keeping the boogeyman at bay

Whether implanted for medical reasons, for employment verification, or simply for convenience or entertainment, these devices pose interesting and real security and privacy risks (not to mention the obvious physical risks associated with using untested and unapproved devices). **While security of implanted devices is clearly important, it alone is not enough to protect a potential victim against attacks or misuse. Technical controls may address the secure storage or transmission of data, but are not useful when applied to purpose, minimization, choice, and accuracy — all critical privacy principles.**

In the world of privacy, certain core principles appear again and again, whether in legislation like the forthcoming European Union's General Data Protection Regulation (GDPR) or through recognized industry standards suggested by bodies such as the US Federal Trade Commission. As the device and the body merge, close adherence to these principles is even more important. Let's consider a few interesting examples in the context of implanted devices:

- **Privacy by design and by default:** Anticipate all potential use and misuse of information, such as the serial number on pacemaker or clearances to trade secrets found in locked offices and build in safeguards like two factor authentication or other command validation criteria. What happens if the network goes down, the device malfunctions, or the manufacturer ceases production? Some developers are exploring using secondary and unique biometric features for authentication such as a patient's individual heartbeat as a

cryptographic key. Privacy by default is related to Privacy by design, but also critical in its own right because of the difficulties changing settings on implantable devices. Once inserted, the “on/off ” switch cannot be simply toggled to change a setting. Data collection must begin only after clear, affirmative action by the host that displays true consent, so the default of connectivity should be “off ” until enabled. This might be established through a secondary interface on a computer, app, or other smart connected device.

- **Purpose:** Consider not just what is possible, what “can” be done, but also what “should” be done. **Is there a legitimate need for all the data collected? Simply because an implantable device can monitor for blood sugar levels for example, does not mean that it should also perform random drug tests on the same sample just because it is possible.**
- **Minimization:** Resist the temptation to collect personal information that is sensitive but unnecessary for the purpose. For example, a chip in a badge might be useful to verify identities and access certain facilities, but collecting all the geolocation of an employee throughout the day — or weekend — is probably excessive and only increases the risk of harm should the data be stolen or lost.
- **Accuracy:** Because of the personal nature of these devices, it might be tempting to treat the data as infallible. Reducing manual data entry improves accuracy, but can lead to catastrophic results if there’s an inaccurate reading. An electronic pulse or a dose of medication might be fatal if delivered at the wrong time. Allowing access to a sensitive lab area to someone that has nefariously stolen data from a legitimate employee’s RFID chip using wireless hacking could expose a company to tremendous theft or interruption of business. Procedures to validate data accuracy must be built in, as when a nurse makes you repeat your name and birthdate before administering medication or the security guard checks your employee photo as you pass the scanners.
- **Disposal:** Plan for the ultimate disposal of the device. The greater the volume of data stored, the more appealing a target, meaning the device may be the riskiest at the end of its life. What if the device is no longer needed — the long-time employee is fired or retires, the medical condition is cured? Must the device be physically removed? If not, are there risks in keeping it embedded long term? Class actions have been brought when implanted medical devices were found to emit toxic levels of chemicals over time; so too might legal risks and liabilities arise with unintended, long-term storage of data. Imagine a cyberattack targeting a company’s entire long-term engineering department. Can the device be remotely wiped, encrypted, or backed up to protect against loss of data stores or cyberattacks like ransomware?
- **Retention:** There are many questions relating to the data collected by an implantable device. Depending on the device, the user base and number of elements being gathered, the volume of data may quickly become overwhelming. With other principals like purpose and minimization in mind, manufacturers must consider how much data needs to be kept and what controls users will have to delete (or request deletion of) data or to otherwise set retention parameters. If a user can elect to discontinue the activity or “connected” capabilities of the device, is the data automatic all deleted or does a user have secondary responsibilities to ensure that their information is destroyed?
- **Global compliance:** The laws applicable to the collection, use, and processing of personal information vary from country to country, state to state, and province to province. Complying with these complex, ever-changing laws keep privacy professionals on their toes. Failure to comply can result in fines large enough to shutter even the largest company and criminal penalties that include prison time. Depending on the data to be collected, multiple laws might impose varying requirements on a device manufacturer, service provider, or data host. The privacy challenges that already exist in a mobile, connected world are made even more

daunting when the device is a ghost: invisible, inseparable, and able to travel anywhere its host might go.

These examples illustrate just a few unique questions raised by implantable technology. While much of this technology is still the stuff of horror novels and the individual risks are low, the one thing we can be sure of is that next Halloween there will be even more scary stories to keep us up at night. Why? Because these implantable technologies are multiplying with the rapidity of zombies. To keep us safe as we venture out in the dark, security and privacy must work together to provide for the protection of the data, the device, and the host, particularly as more technology is pushed deeper under our skin.

Karen McGee

Privacy and Security Lawyer

Intel

She is also a member of the compliance & ethics and IT, privacy & e-commerce committees and a member of the big data subgroup.