Published on *The National Law Review* https://natlawreview.com

Privacy Fashion: Profit from the Surveillance State

Article By:

Theodore F. Claypoole

Privacy has never been fashionable in this country. The Europeans and Canadians seem to care so much about it, and, as well documented in my earlier Heydatadata posts this month, Americans by the millions are sending their DNA to private companies or weight loss factories without any concern at all.

We put Progressive Insurance spybots in our cars on the off chance we might somehow save money. We bring always-on listening and recording devices into our homes. We allow random app providers to track all of our movements through smartphones.

But this trend seems to be changing. The new privacy law in California is beginning to acclimate consumers to think about how their data is used. Other state legislatures are currently piling on to the privacy protection trend. Enough people in this country are becoming nervous about the information collected online, captured by wearable tech, tracked by our smartphones, surveilled by our home appliances, that many are expressing concern to me. Some are even panicked about it.

Where there is panic and concern, there is money to be made. And I think we are on the cusp of an explosion in demand for products that shield us from all the prying, probing, pulling signals flying from us, projected at us, and surrounding us. Attention please. If someone starts making inexpensive tools to protect us from the surveillance state, I believe that person will sell many and profit big.

The great tech writer Kashmir Hill, whom I recognize from years of reading her terrific stories on privacy and the tech industry in Forbes, and who now seems to be writing for the New York Times (congratulations on the step up, Kash), just dropped a great article on Anti-tech tech. In it she describes the nascent research and industry for blocking the tools that capture our most intimate information.

The star product is the Bracelet of Silence developed at the University of Chicago. The chunky metal wearable uses 24 speakers “that emit ultrasonic signals when the wearer turns it on. The sound is imperceptible to most ears, with the possible exception of young people and dogs, but nearby microphones will detect the high-frequency sound instead of other noises.”

In other words, your Amazon Echo or Google Home devices can’t hear what you are saying, and they are listening more often than you think and recording everything they hear. Neither can your cell phone (“Siri, stop spying on me”) or probably other random listening devices left resting in the retail

isles, hotel lobby or office. All in all, a terrific tool for people who don't know what tech is listening and who wish to squelch the recordings before they can start. The bracelet of silence can be switched off and on as needed.

And for those of us who are deeply paranoid and/or the objects of intense and directed surveillance (just because you're paranoid doesn't mean they are not spying on you) this device should also thwart anyone who turns on the microphone of your smartphone to hear your conversations or who plants listening devices in your vicinity. Intended to stop casual listening, it may also be used to kill more intentional spying. I want one.

But we can't have one right now. Ms. Hill reports, "At this point, the bracelet is just a prototype. The researchers say that they could manufacture it for as little as $20, and that a handful of investors have asked them about commercializing it." Good readers take note. This opportunity is still available to dynamic entrepreneurs. And if you focused on the stylishness of the wearable device you could have a viral hit on your wrist.

The article also talks about other early examples of protective wearables, from those that shield the RFID chips in your wallet to an art project that masks heat signatures to hide you from passing drones. Any of us can purchase counter surveillance spy gear that can block RF signals or find tiny camera lenses.

For several years, researchers and entrepreneurs have been working to develop wearable tools to thwart facial recognition systems. The NY Times article featured here discusses reflectacles, "a line of reflective frames that turned back visible and infrared light. When a surveillance camera films a person wearing the $164 frames, the reflected light blurs out the face."

Other options include a shirt imprinted with many people's faces to confuse recognition systems, and anti-recognition hair and make-up products. Once again, an inexpensive and fashionable set of these tools is likely to appeal to many of us, not just people out to confound the law.

Kashmir Hill's best known NY Times story to date has been her page 1 expose of Clearview AI, a shadowy company paid by more than 600 law enforcement agencies (and other companies) using facial recognition of private individuals taken from the web. The article quotes, "The weaponization possibilities of this are endless," said Eric Goldman, co-director of the High Tech Law Institute at Santa Clara University. "Imagine a rogue law enforcement officer who wants to stalk potential romantic partners, or a foreign government using this to dig up secrets about people to blackmail them or throw them in jail." No one seems to be slowing this march of casual surveillance on the macro level. We may need solutions on the individual level.

As the internet of things grows in number of devices – and there may be more than 75 million of them by 2025 – we will be seeking more ways to remain unobtrusive in an environment tracking our every move and sending that information to governments, businesses and probably even people in our lives. Privacy wear is likely to be an entire category of fashion. I am surprised that the Europeans don't have a fully blossoming privacy fashion industry organized already.

National Law Review, Volume X, Number 51