Beacons: Your Phone Is Listening To Your TV – Literally!

TN Note: Surveillance more sophisticated than ever before, and in ways that you would never expect. Read this to understand how your phone can detect hidden tones coming from your TV to identify you and both of your devices as belonging to you. In the hands of a technocrat, this kind of spying has a dark ending.

The TV is on in the background, and you're replying to a quick email on your phone nearby. You don't know it, but the devices are communicating. During a commercial, the TV emits an inaudible tone and your phone, which was listening for it, picks it up. Somewhere far away, a server makes a note: Both devices probably belong to you.

This information about which devices belong to whom is immensely valuable to advertisers hoping to target ads specifically to you. In a simpler time, targeted marketing was easy. Most people had a computer at work and maybe another at home. If you sent an email about your new cat, ads for cat food started cropping up. If you searched for Thanksgiving recipes, Safeway coupons for turkeys appeared in your Facebook newsfeed.

Those were good days for advertisers tracking Internet users. It wasn't so hard to find what people were up to online, because most routinely used just one or two connected devices.

But now, between laptops, phones, tablets, wearables, and Internet-enabled cars and TVs, advertisers have access to more information than ever before for ad targeting. They just need to figure out which devices live under the same roof.

That's harder than it sounds. Unless you're logged into a service on all your devices—for example, by using Google's various services everywhere—advertisers need to get creative to stitch together a portrait of you.

Verizon's "supercookies"—a snippet of code injected into mobile users' web requests—silently identify and track its customers, sharing the information with AOL's wide-reaching ad network. Vizio Smart TVs tie customers' viewing habitsto a home Internet address and sell the information to advertisers. And both programs require customers, who are often unaware of the programs, to opt out of them if they don't wish to be tracked.

But a newer method of cross-device tracking wanders into the realm of science fiction. According to a filing from the Center for Democracy and Technology, a digital human rights and privacy advocacy organization, companies have figured out how to use inaudible sounds to establish links between devices.

Here's how software from SilverPush, a leading provider of "audio beacons," works: When you visit a website that uses SilverPush tracking technology, the site causes your device to emit an inaudible ultrasonic

sound. If any other devices you've got lying around—a laptop, a phone, a tablet—has an app installed that includes SilverPush code, it's listening for that sound. If it hears it, SilverPush knows that the two devices are close to one another and, presumably, belong to the same person.

Read the full article here…