Forbes http://onforb.es/1DXXUno

Sarah Jeong Contributor

I write about the law, technology and the free flow of information.

Opinions expressed by Forbes Contributors are their own.

TECH 10/28/2014 @ 4:31PM | 245 views

Surveillance Begins at Home

Comment Now

As Domestic Violence Awareness Month comes to a close, we ought to have a conversation about how technology aids and abets intimate partner violence. Privacy advocates rarely connect the dots between intimate partner violence and surveillance, and anti-violence advocates often fail to talk about technology in its entirety—and they omit in particular the complicity of law enforcement in the abuse of technology.

Only a handful of articles and other reports hint at a widespread problem. For example, this NPR segment found a pattern among shelters:

> NPR surveyed more than 70 shelters — not just in big coastal cities like New York and San Francisco, but also in smaller towns in the Midwest and the South.
>
> We found a trend: 85 percent of the shelters we surveyed say they're working directly with victims whose abusers tracked them using GPS. Seventy-five percent say they're working with victims whose abusers eavesdropped on their conversation remotely — using hidden mobile apps. And nearly half the shelters we surveyed have a policy against using Facebook on premises, because they are concerned a stalker can pinpoint location.

This piece in BetaBoston, which features a chilling personal story, also interviewed Andrew Lewman, the executive director of the Tor project, who touts Tor as a useful tool for shelters and social workers.

> For example, one abuser might hack a company's password database and share the whole thing with others online, Lewman said. Digital communities have sprung up where individuals teach each other how to compromise cell phones to track victim's whereabouts, listen to conversations in a room, take pictures, and read texts and email so that they can learn about their victim's behavior on a microscopic level.
>
> Often the language to describe the surveillance is couched in protective terms, such as monitoring a child's activities or queries posed to check if a partner is cheating. Commercially available software advertises easy tracking of exact locations, call logs, text messages, and more, often in an interface as easy to use as Google Maps.
>
> And while digital stalkers often know nothing more about technology than the average person, their devotion is intense.
>
> "Most of them quit their jobs and do this full time or they've been fired," Lewman said. "They spend all their time thinking about what they're going to do next."

No doubt the second paragraph is referring to how spyware like StealthGenie is marketed. Stealthgenie's creator was arrested in September. Kashmir Hill here at Forbes wrote:

> The app's website advertised its use for monitoring "employees and loved ones such as children," but according to the FBI, Akbar and his team developed an internal business plan that revealed that — duh — the primary target audience for the app was people who thought their partners were cheating.

The formulation "people who thought their partners were cheating" downplays the likelihood that that the app was used as part of a larger pattern of abuse. To my knowledge, the connection between specific spyware applications, keyloggers, and so forth, and intimate partner violence has not been studied. But we know that women keep showing up to shelters with compromised devices. We know that the National Domestic Violence Hotline website advises visitors who are victims to call, rather than browse the site.

Screenshot of National Domestic Violence Hotline Website

Intimate partner violence does not only happen to women, but the hard statistics make it a women's issue. Women make up 4 out of every 5 victims of intimate partner violence. And women are also disproportionately murdered by intimate partners. About a third of female homicide victims over the age of 12 are killed by an intimate partner, where about 3% of male homicide victims are killed by an intimate partner.

I don't bring this up as an obligatory footnote to a discussion about intimate partner violence. The gender skew directly affects how we understand remedies and solutions. It's not enough to acknowledge that technology is used by abusers, and then to progress directly to "And that's why police need to address this new menace!"

Police officers as a body are overwhelming male. They are also more likely to commit intimate partner violence than the general population. Some sources say that police officers are four times more likely to commit domestic violence; others say twice the average rate. Combine this knowledge with the knowledge that technological surveillance is used against victims of intimate partner violence, and suddenly the law enforcement abuse and promotion of surveillance technologies begins to sound more sinister.

We don't know much about police abuse of women through police surveillance tools. But we do know that inside the NSA, officers abused their power to spy on loved ones, so much so that the phenomenon had a cute

nickname inside the agency: LOVEINT. We also know that at the NSA, intercepted nude photos were shared as a "fringe perk." We know that the California Highway Patrol have made a "game" out of stealing nude pictures from female arrestees. We know that Gilberto Valle, the "Cannibal Cop," used his access to a law enforcement database to stalk potential victims. We know that Valle probably isn't the only one; using federal databases to stalk women might be quite common for all we know—see *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir.), in which the defendant accessed the information of 17 different women, and later showed up suddenly at some of the women's houses. We know that the celebrity nudes were hacked through a brute force attack achieved by a police tool. We know that local police departments around the country promote software called ComputerCOP, a keylogger (software that logs everything that gets typed on the computer, and gives that information to the attacker).

With this information in the background, FBI Director Comey's insistence that Apple's new iPhone encryption will undermine law enforcement becomes less farce, and more tragedy. As women's shelters across the country have learned, privacy tools are not just for journalists, whistleblowers, spies, and criminals.

About 12 million people are victims of intimate partner violence each year. Privacy is about power, and undermining privacy serves the powerful at the cost of the powerless, even at home. For an unknown number of people, surveillance is not an exotic threat, a national story, a geopolitical game. For them, surveillance begins at home.
