Creepy And Dangerous: Facebook's 'People You May Know' Gone Invasive

This story is not about sex workers, but rather about how Facebook is mining external, non-Facebook data to merge with member profiles, and then exposing that to the world. There are huge legal and ethical issues, but who hasn't been creeped out when certain people pop up on y our 'People you may know' list in Facebook? Now you have a glimpse into what they are doing, and how it can be tremendously dangerous. TN Editor

Leila has two identities, but Facebook is only supposed to know about one of them.

Leila is a sex worker. She goes to great lengths to keep separate identities for ordinary life and for sex work, to avoid stigma, arrest, professional blowback, or clients who might be stalkers (or worse).

Her "real identity"—the public one, who lives in California, uses an academic email address, and posts about politics—joined Facebook in 2011. Her sex-work identity is not on the social network at all; for it, she

uses a different email address, a different phone number, and a different name. Yet earlier this year, looking at Facebook's "People You May Know" recommendations, Leila (a name I'm using using in place of either of the names she uses) was shocked to see some of her regular sex-work clients.

Despite the fact that she'd only given Facebook information from her vanilla identity, the company had somehow discerned her real-world connection to these people—and, even more horrifyingly, her account was potentially being presented to them as a friend suggestion too, outing her regular identity to them.

Because Facebook insists on concealing the methods and data it uses to link one user to another, Leila is not able to find out how the network exposed her or take steps to prevent it from happening again.

> *"With all the precautions we take and the different phone numbers we use, why the fuck are they showing up? How is this happening?"*

"The worst nightmare of sex workers is to have your real name out there, and Facebook connecting people like this is the harbinger of that nightmare," she said. "With all the precautions we take and the different phone numbers we use, why the fuck are they showing up? How is this happening?"

It's not a question that Facebook is willing to answer. The company is not forthcoming about how "People You May Know," known internally as PYMK, makes its recommendations. Most of what Facebook does reveal about the feature is on a help page, which says that the suggestions "come from things like" mutual friends, shared networks or groups, or "contacts you've uploaded."

When the suggestions turn out to be unnerving, that explanation is both vague and woefully incomplete. A Facebook spokesman told me this summer that there are more than 100 signals that go into PYMK. All someone like Leila—who was not connected to her clients by anything like mutual friends, networks, groups, or contacts—can know is that the data that exposed her must be something else, in that large undefined set of factors.

Leila suspects either that Facebook collected contact information from other apps on her phone or that it used location information, noticing that her and her clients' smartphones were in the same place at the same time.

Read full story here…

Blockchain? Trump Admin Seeking Alternatives To Social Security Numbers

Calls for a universal ID system has skyrocketed since the Equifax breach and Technocrats are chomping at the bit to uniquely identify everyone, everywhere. This leapfrogs the concept of RealID by a country mile, and would be twice as dangerous to privacy. TN Editor

On October 4, 2017, following the extensive security failure of Equifax Inc., reports indicate that the Trump administration is exploring

alternatives to the standard means of identity provenance: Social Security numbers.

Special assistant to the president and White House cybersecurity coordinator Rob Joyce spoke Tuesday at a Washington cyber conference on what he described as an outdated identity system. "I feel very strongly that the Social Security number has outlived its usefulness. Every time we use the Social Security number, you put it at risk."

In light of the fact that 143 million US customers' private information was accessed by hackers, the 45th presidential administration is leaning on other federal departments to help find an adequate replacement for the existing system, while exposing its weaknesses.

Appearing before the House Energy and Commerce Committee in an effort to offer an explanation for the hack was Equifax CEO Richard Smith, who was the recipient of admonition from both sides of the political aisle. Smith faced questions regarding the scale of the data breach and why Equifax executives failed to act swiftly to disclose the information. Mere days after the hack, three CEOs of Equifax sold shares worth $2 million (according to the SEC) but claim to have had no knowledge of the attack.

Smith pointed to a growing number of hackers who are targeting Social Security numbers as evidence of their vulnerability. He said:

> *"The concept of a Social Security number in this environment being private and secure – I think it's time as a country to think beyond that. What is a better way to identify consumers in our country in a very secure way? I think that way is something different than an SSN, a date of birth and a name."*

Joyce indicated that a better system would include the implementation of a "modern cryptographic identifier," going on to say, "It's a flawed system that we can't roll back that risk after we know we've had a compromise. I personally know my Social Security number has been compromised at least four times in my lifetime. That's just untenable."

Examples that harken back to Estonia's digital identity program were made by Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology in Washington, as he described a system wherein a "physical token," embedded with a private key, could be issued to individuals in conjunction with a PIN. This would allow citizens to establish that they were who they claim to be, the same way one would with a debit card.

"Your pin unlocks your ability to use that big number [or private key]," said Hall, who acknowledged that while "it's very promising" as well as technically feasible, it is still a "pretty big endeavor," with a substantial cost for deployment to every US citizen.

Bob Stasio, fellow at the Truman National Security Project and former chief of operations at the National Security Agency's Cyber Operations Center, pointed to blockchain technology as a means of creating numbers that are mathematically impossible to maliciously replicate. Rather than relying on a numeric system that was implemented in 1936, blockchain technology can provide "a much more efficient and mathematically sound method of transaction, identification and validation."

Read full story here…

Selective Censorship: Apple Pulls Pro-Life Group's App From App Store

Selective censorship by media giants is increasing at an alarming speed: if they don't like your politics or morality, they simply push the 'eject' button and you disappear. Technocrats have no ethical boundaries in censorship because they believe so strongly that they are right and everyone else is wrong. TN Editor

After the social media giant Twitter came under fire for censoring a pro-life ad, another huge media icon is facing criticism.

This time, a pro-life group tells LifeNews that Apple approved and subsequently removed its app from the App Store after criticism from abortion activists and liberal media outlets. As Human Coalition informs LifeNews, it released a mobile app allowing pro-life individuals and church groups to pray for Human Coalition's abortion-seeking clients,

who remain anonymous, in real time. The app, "Human Coalition," was available for android devices in the Google Play Store, and in the Apple App Store for iOS.

After that, this past summer, the pro-life group came under intense public criticism as pro-abortion journalists took notice of the app and began attacking Human Coalition for urging pro-life people to pray for women contemplating abortion. Some articles falsely accused Human Coalition of making public women's private information.

Left-wing writer Christina Cauterucci at the pro-abortion blog Slate wrote:

> *With the help of an app developed by the anti-abortion Human Coalition, it was easy! I saved real-live babies from the clutches of money-grubbing abortion providers with just a couple dozen swipes of my right thumb, as if I were paging through Tinder or wiping a little schmutz off the screen of my phone.*
>
> *You too can be a baby-saving hero. Your superpower awaits at your favored app store, searchable under "Human Coalition."*

And Amelia Tait at the U.K.'s The New Statesman wrote:

> *Are digital anti-abortion prayers sanctioned by the church? Do they reach God? Though these questions may seem faintly ridiculous, their answers seem more important than ever. When it comes to the tech behind these anti-abortion apps however, that is where people – religious or not – might do well to lose a little faith.*

That's when Human Coalition tells LifeNews the problems began.

"In July, on the heels of pro-abortion media pushback, Apple notified us that they had removed the Human Coalition app from the App Store, citing violations of certain functionality requirements. However, Human Coalition spoke with Apple and demonstrated that not only were the cited requirements met, but that the Human Coalition app exceeded minimum requirements and functioned better than similar apps from other developers," it said.

It added: “Apple was unable or unwilling to identify a specific improvement that, if completed, would merit the Human Coalition app’s reinstatement in the App Store. Instead, the effect of Apple’s requirements for modifying the app before it could be re-submitted for consideration would be that Human Coalition would have to completely overhaul of the app — a cost-prohibitive and unnecessary demand.”

“Just weeks after Apple removed our pro-life app from the App Store, abortion activists announced a targeted campaign aimed at stopping our pro-life work in the city of Atlanta. The Netroots Nations conference, with sponsorship from the abortion industry and major corporate backers including Google and Facebook, included in its agenda a protest of Human Coalition’s Atlanta clinic, the group continued.

The pro-life organization says this is another in the latest trend of media outlets and abortion advocates pushing to silence pro-life views.

“Censorship of pro-life voices is a growing trend in the United States. Pro-abortion media, for their part, have demonstrated time and again their willingness to reinforce bogus and false narratives about pro-life Americans, going so far as to try to bully pro-life voices into silence. Human Coalition will continue rescuing children from abortion and serving women and families until abortion is unthinkable and unavailable in our nation,” it concluded.

Read full story here…