OPINION

5 shocking new threats to your personal data

I don't mean to alarm you, but these trends make panic sound like a good idea

By Mike Elgan | Follow

Contributing Columnist, Computerworld FEB 4, 2017 4:00 AM PT

I'm not paranoid. Tinfoil hats aren't my scene.

But watch out! In just the past month, the internet and smartphones have come up with five new and surprising ways to steal or expose our personal data.

Of course, these new concerns can now be added to all the old ones. Companies like Google and Facebook still track you and harvest personal data. Hackers still want to steal your data. And the National Security Agency is still out there doing its thing.

And now, these five new trends reveal that your security and privacy could be compromised in ways you probably never imagined.

1. Fingerprints can be stolen from selfies

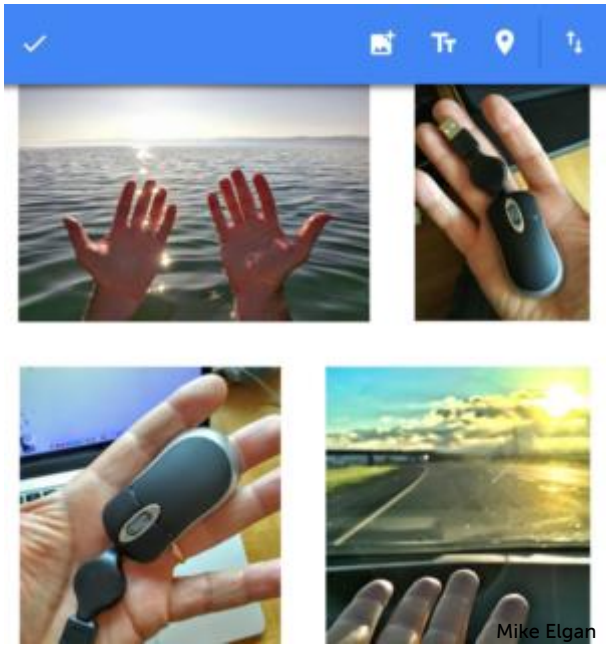
Researchers at Japan's National Institute of Informatics (NII) announced recently that your fingerprints could be stolen from photos of your fingers, and the prints could then be re-created and used to bypass biometric security systems.

Smartphone cameras have gotten so good, so high-resolution, that the ridges and valleys that make up your unique fingerprints could be copied and used to foil fingerprint security schemes.

This is a special threat for Japan, where flashing the "V sign" or "peace sign" with the hands is a common gesture in photographs posted online.

Skeptics are skeptical. For starters, the "researchers" were hawking a ridiculous "solution" to the problem -- a clear titanium oxide film with a specific pattern printed on it that you would somehow place on your fingers to cover your prints before taking a selfie.

Also: Conditions have to be just right. The fingers must be in focus, the lighting must be perfect, the distance from the camera must be about nine feet and the photographer must use a very high-end smartphone. (And such phones typically focus on the face, not the fingers.)



The high-resolution versions of photos like these of the author's own hands could be used to copy fingerprints.

But I think the skeptics are wrong. You should worry.

First, fingerprint-photo theft has already been demonstrated. Two years ago, a German named Jan Krissler re-created the fingerprints of German defense minister Ursula von der Leyen from publicly available photos and made a 3D mold of her finger that could unlock a smartphone.

Second, the technology already exists. No additional research is necessary.

Third, fingerprints are forever and cannot be changed, so stealing fingerprints isn't like stealing a password, which can be changed.

Fourth, smartphone cameras keep getting better. It's only a matter of time before most people carry cameras at least as good as the best found in the iPhone 7 or the Samsung Galaxy S7.

And finally, hackers can use online photos as the starting point, rather than targeting specific people. It could be difficult to target a specific person, because you'd have to go looking for high-quality photos of that person's fingers. But if your starting point is all the high-resolution photos of fingers on, say, Google Images, then you could potentially harvest hundreds of thousands of prints efficiently.

I've scanned my own private Google Photos trove and found plenty of fingerprint-friendly photos. If I had made them public, a malicious and resourceful person could use multiple photos to re-create my fingerprints.

2. Political trolls 'win arguments' by publishing your personal data

In this heated political season, with vitriol lobbed from one filter bubble to the next, acrimony rules the social web. The latest trend in online political arguments is doxing, which is the act of exposing someone's personal information online.

Some kinds of information, such as phone numbers and home addresses, are easy to find online and also conducive to harassment. One hater doxes, and a hundred others call with death or bomb threats or engage in swatting, where you call the police and falsely report that a violent confrontation is underway at someone's home, leading the police to send the SWAT team to that address.

The problem recently got so serious on Reddit that the site deleted and banned the r/altright and r/alternativeright subreddits. Reddit was unable to curb doxing in the subreddits in the usual ways, so it resorted to the nuclear option and terminated them.

Sadly, doxable personal information is trivially easy to find online because...

3. Genealogy sites have already posted your personal information online

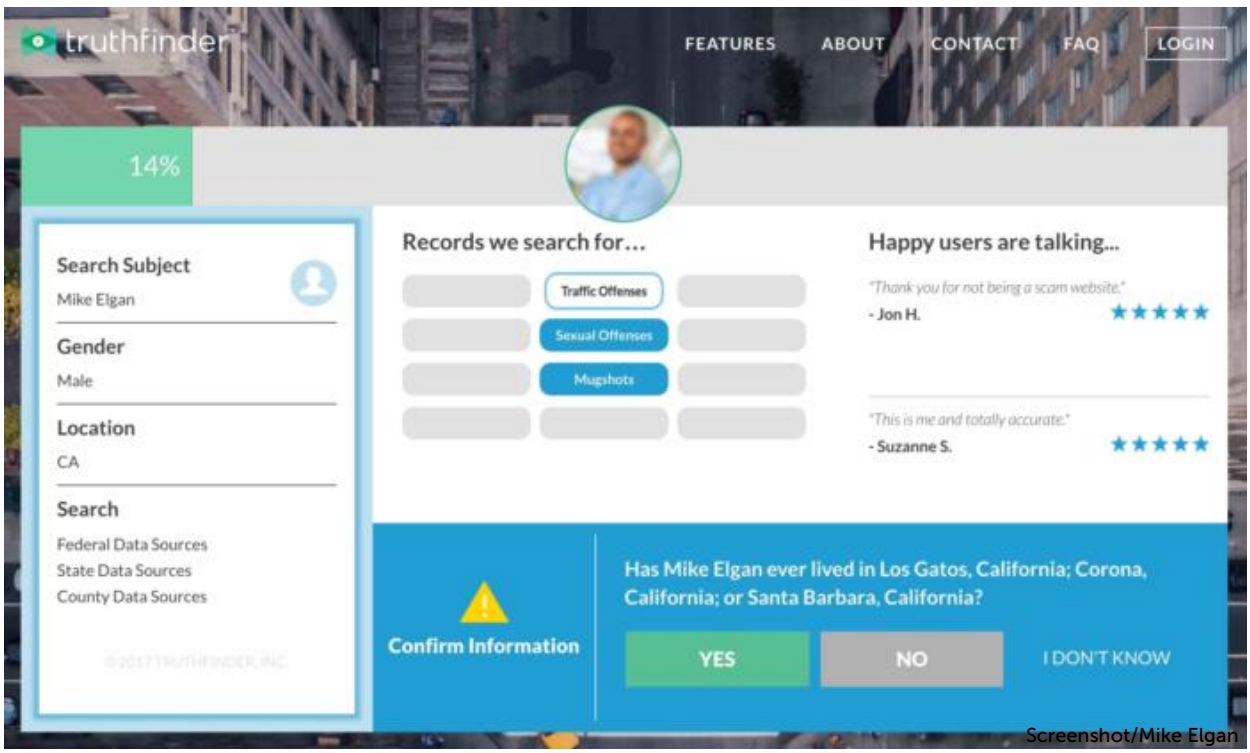
Personal information sites, including genealogy and "people search" sites, have been around for years.

The business model has long been to tease people with the kinds of information the sites could provide them and require interested parties to pay to get the full set of data.

But now, two trends have popped up that should freak you out.

The first is the emergence of a personal information super site called Family Tree Now. The site gives away free the kind of information that others have been charging for. This caused a great deal of concern last month after a woman tweeted about the previously obscure site. If you simply enter a name and the state where that person lives, Family Tree Now can often tell you the individual's other family members, along with their ages and current and previous home addresses.

The second trend is that some "people search" sites use social engineering to get you to give them information, instead of the other way around. For example, the site TruthFinder asks questions throughout the process, claiming that your answers will help it give you better data. In fact, TruthFinder is getting information from you.



Some "people finder" websites make a dramatic show of searching databases to tell you information about someone — but as they do that, they pepper you with questions so they can add your answers to their databases.

4. Mobile apps send personal data back to a remote server

A Chinese selfie-editing iPhone app called Meitu transforms your face into a surreal cartoon image that whitens, brightens, enlarges the eyes and adds visual effects.

Two weeks ago, the app exploded in popularity because the effects are so unusual and over the top. It turns your face into a dreamy cartoon character. But overnight, it emerged that the app sends all kinds of information back to China, including your location, details about your mobile carrier and IP address, and the IMEI numbers of Android users. The company responded to online outrage by saying it doesn't sell the data and uses it only to improve the app.

The controversy raised awareness about an uncomfortable fact, which is that many apps harvest your data without your knowledge or explicit permission.

So what's the solution? Security apps? Unfortunately...

5. Even security apps can threaten your security

One of the best ways to protect one's privacy online is to use a VPN, or virtual private network. VPNs theoretically let you use the public internet as if you were on a private network. They let you hide and encrypt your online activity, even from your own ISP. And they enable you to spoof your location, so you can say you're going online in another city or country.

However, a recent study found that an alarmingly high number of VPN services offered through Android apps violate your privacy, rather than protect it.

The study, conducted by researchers at the University of South Wales in Australia, found that 38% of Android VPNs are infected with malware, 18% don't have encryption and 75% track user activity. Some Android VPNs inject JavaScript programs for tracking or for redirecting online shopping queries to paid partners of the app creator.

What to do about the new privacy and security threats

You've heard the standard best practices for protecting your privacy. Turn on two-factor authentication whenever and wherever you can. Use a password manager like LastPass. Download apps only when they've been recommended by a credible authoritative

Because of these new threats to privacy and security, I would recommend the following additional steps.

First, sign up for a site called "Have I Been Pwned?" It will alert you when your personal information shows up online as the result of a hack. Often hackers crack a site, download all the user data, then post it or sell it on the dark web.

Second, try to think of all the sites you signed up for but later abandoned. Go back and actively delete your account.

Third, consider disinformation. Whenever a site wants personal data, give fake information. If your information gets hacked, doxed or exposed, your real information won't be used.

Fourth, search through your photos looking for images of hands and fingers and make sure no usable fingerprints exist.

Fifth, don't get into heated arguments with trolls, haters or political extremists online.

Sixth, go to Family Tree Now and remove your personal information.

The internet is always coming up with new ways to violate your privacy and security. But you can fight back.

A little paranoia goes a long way.

To express your thoughts on Computerworld content, visit Computerworld's Facebook page, LinkedIn page and Twitter stream.

Mike Elgan writes about technology and tech culture. Contact Mike and learn more about him at http://elgan.com/about.

SHOP TECH PRODUCTS AT AMAZON