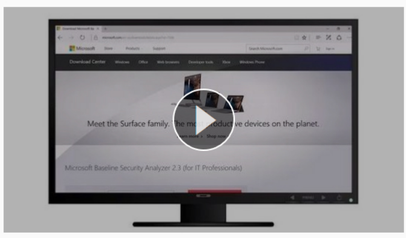
With my cell-phone number, a private eye found 150 pages on me

Steven Petrow, Special for USA Today Published 10:43 a.m. ET July 21, 2017 | Updated 9:27 a.m. ET July 24, 2017



USA Today columnist Kim Komando guides you on how to test your computer's security.

(Photo: Getty Images)

RTCOur cell phone numbers are increasingly used for identity theft, the modern-day linchpin to most personal data.

Now I know that first hand.

After reporting on how phone number identity theft had doubled last year, and warnings about how cell-phone numbers are being used as the new Social Security numbers, I wanted to see how much was at stake.

I gave my cell number to private investigator Thomas Martin, a former federal agent and now president of Martin Investigative Services in Newport Beach, Calif., and asked him to do his thing. A few days later a three-pound, 150-plus-page dossier arrived at my front door via FedEx. Martin didn't trust regular mail given the nature of what it contained, which was tons of my private information.

"We didn't even scratch the surface," Martin told me later. He also made a point of telling me that I was "cleaner than a Safeway chicken."

Starting with just my cell phone number, Martin had obtained my full name, Social Security number, and date of birth. Then came my home address—and every address I've had since college. How much I'd paid for my house, the amount of my mortgage, my annual property taxes, even my driver's license number and the Vehicle Identification Number of my car – all in there. The *pièce de résistance*, if you want to call it that: A financial overview that includes bankruptcies, liens, foreclosures, and judgments. (I didn't have any.)

These days you have to protect your phone number like you do your Social Security number. *(Photo: Getty Images)*

Martin also put together a list of my social media pages. In the interest of time he did not do a detailed search, but easily could have; employers regularly engage the company to do just that about new recruits and employees. If there had been a picture of me at a gay nightclub (yep, I'm gay) he could have found that, too, and some employers might use that to fire me (and in some two dozen states it would be perfectly legal to do that). "If you're on porn sites, we're probably going to find it," he added.

He also searched for "possible criminal records," turning up two leads.

In his search, which he told me several times was completely legal, Martin could determine if I had any hunting and weapon permits and whether I was on a global watch list. Chillingly, my dossier included significant information about "possible relatives" and "likely associates." That would be my parents, my siblings plus their spouses and kids, other family members and neighbors. There was information about the mother of one of my sisters-in-law, a woman who died 15 years ago. In short, the database search on me retrieved information about this distant relative all the way back to 1975—42 years ago. The point: Data lives forever, even though we don't.

I also spoke with Eric Vanderburg, director of information systems and security at Jurinnov, LLC, a data security firm for the legal and business communities. I wanted his take on the data Martin found. "Once a phone number is included in this digital information trail, it becomes part of the package and can be used to find all the other information about that person. That information is available to anyone who wants it at a cost," he explained.

How much, I wondered. Martin told me that his services start as low as $350 to verify identity, with full searches like mine usually costing $950. (Disclosure: Martin did not charge USA Today for the cost of my search.)

Fortunately the federal Privacy Act of 1974, the Fair Credit Reporting Act, and some state laws provide a bit of shade to a few bits of our personal data. My tax returns weren't in the dossier, and since federal law prohibits the release of educational information, the packet included nothing about my schooling. I guess that was some small relief.

But … everything in those pages was discovered legally. Martin was playing by the rules, but bad guys don't. Vanderburg explained that criminals "maintain [their own] databases of information on potential targets," because purchasing the information would leave a paper trail. These databases, Vanderburg said, may contain information that is illegal to collect, "such as former or current passwords," explicit photos, personal data files, contact lists, and more."

And the core of all of this is your cell phone.

"I could never get your social media stuff with just your Social Security number," Martin pointed out – because users aren't asked to provide it when setting up new accounts. We are, however, asked for our phone numbers, which is why certain indexes are only tied to the cell phone number.

What to do:

Beware of passive disclosure. We're constantly divulging our own data, clicking "yes" to agreements that give up our phone numbers, search history, geolocation information, IP address, computer operating system, and ads clicked on. Don't let convenience overshadow security. Most of the time we don't even know what we're revealing.

Be stingier about active disclosure. Mail-in rebates, product registrations, coupons, credit requests, and discount cards often ask for a phone number. Vanderburg warns that "this information is stored in databases and sold," and too often, it's hacked.

Don't play around. What Pokémon character are you? What would your *Star Wars* name be? What celebrity do you most resemble? You're likely to be lured into divulging information that can come back to haunt you, Vanderburg said.

My last piece of advice: Every time you're asked to give up your cell phone number, ask this: "What would I do if the request were for my Social Security number?" If you wouldn't give that number out, don't disclose your phone number.

Oh, as for those criminal records that came up in my search. The good news: both were for traffic infractions. The bad news: the database doesn't indicate that. By the time I might get to explain myself to a potential employer, admissions officer, or a new romantic interest, they may have moved on—leaving me behind.

USA TODAY columnist Steven Petrow offers advice about living in the digital age. Submit your question at stevenpetrow@gmail.com. You can also follow Petrow on Twitter: @StevenPetrow. Or like him on Facebook at facebook.com/stevenpetrow.