CNET News
Security
August 17, 2009 6:01 AM PDT

How 10 digits will end privacy as we know it

by Ari Juels

Editors' note: This is a guest column. See Ari Juels' bio below.

Internet denizens and urban dwellers alike need to recognize that an era of anonymity is ending.

The population of the world stands at about 7 billion. So it takes only 10 digits to label each human being on the planet uniquely.

This simple arithmetic observation offers powerful insight into the limits of privacy. It dictates something we might call the 10-Digit Rule: just 10 digits or so of distinctive personal information are enough to identify you uniquely. They're enough to strip away your anonymity on the Internet or call out your name as you walk down the street. The 10-Digit Rule means that as our electronic gadgets grow chattier, and databases swell, we must accept that in most walks of life, we'll soon be wearing our names on our foreheads.

A study of 1990 U.S. Census data revealed that **87 percent of the people in the United States were uniquely identifiable with just three pieces of information** (PDF): five-digit ZIP code, gender, and date of birth. Internet surfers today spew considerably more information than that. Web sites can pinpoint our geographical locations, computer models, and browser types, and they can silently track us using cookies. Banking sites even confirm our identities by verifying that our log-ins take place at consistent times of day.

Database dossiers, too, carry surprising amounts of identifying information, even when specifically anonymized for privacy. Researchers at the University of Texas at Austin last year **studied a set of movie-rating profiles from about 500,000 unnamed Netflix**

subscribers (PDF).

Knowing just a little about a subscriber--say, six to eight movie preferences, the type of thing you might post on a social-networking site--the researchers found that they could pick out your anonymous Netflix profile, if you had one in the set. The Netflix study shows that those 10 deanonymizing digits can hide in surprising places.

Our physical belongings also betray our anonymity by silently calling out identity-betraying digits. Small wireless microchips--often called radio frequency identification, or RFID, tags--reside in car keys, credit cards, passports, building entrance badges, and transit passes. They emit unique serial numbers.

Once linked to our names--when we make credit card purchases, for instance--these microchips enable us to be tracked without our realizing it. One popular book inflames imaginations with the lurid title, "**Spychips: How Major Corporations and Government Plan to Track your Every Move with RFID**."

There's little point in hiding the serial numbers of chips when your mobile phone squeals on you.

But wireless microchips also highlight the futility of anonymity protections. To begin with, **concerns about RFID tracking** miss the forest for the trees. After all, mobile phones are ubiquitous and can be tracked at much longer ranges than standalone chips. Many people have GPS receivers in their phones and are signing up for location-based services, voluntarily (if selectively) disclosing their movements. There's little point in hiding the serial numbers of chips when your mobile phone squeals on you.

Many scientists (including me) have developed antitracking techniques for mobile phones and microchips. Instead of fixed serial numbers, wireless devices can call out changing pseudonyms, such as the rotating license plate numbers on spies' **cars** in the movies. The problem is that the plates may change, but the car always looks the same. In this regard, chips are like cars.

Scientists at ETH Zurich **recently showed how to identify microchips uniquely using radio waves** (PDF)--and consequently to see through the disguise of pseudonyms. Their experiments showed that thanks to manufacturing variations, microchips, laptop Wi-Fi cards, and other devices can't help but emit physical "fingerprints"--essentially God-given serial numbers. More digits that we radiate unknowingly.

In the end, we probably won't need to carry anything at all to see our identities betrayed in public spaces. There are already **tens of millions of surveillance cameras in public**

spaces in the United States.

Face recognition software is crude today, but it will improve. Cameras will eventually recognize faces as well as people do. Unlike people, though, they'll have the backing of databases containing millions of faces--or the headshots that so many of us already post online.

Thankfully, despite proliferating sources of those 10 digits that are fatal to anonymity on the Internet and the sidewalk, we can still prevent the world of the film "**Minority Report**." There are many defensible facets to privacy beyond identity. Even if our names are blazoned forth to all and sundry, we still have the opportunity to safeguard health care and financial data, entertainment preferences, purchase histories, and social interactions.

In this battle, **identity theft is a key challenge** for technologists and policymakers. The only way to prevent unauthorized access to personal data is to ensure that even when criminals learn the digital constituents of your identity, they can't steal it. Strong authentication will need to fill the gap as the privacy of identities crumbles.

Perhaps the world will be friendlier when in-store advertisements greet you personally, criminals wear "Hello, My Name Is" badges, and the people you meet at parties already have your bio in hand. Facebook, Twitter, and pervasive blogging already augur a society of reflexive exhibitionism and voyeurism. But the technologies that advance us into a world of omniscience will also bring us a step backward.

For years, people aspired to escape small towns for the big city, for the fresh start of an identity without history. The Internet offered similar horizons of freedom. But the society of the small town will soon have us back in its clutches, for good and bad. And on the Internet, everyone will know if you're a dog.

As chief scientist and director of RSA Laboratories, a security research division of EMC, Ari Juels works to bring sparks of invention and insight from RSA's scientists and affiliates to the company as a whole. Ari, who joined RSA in 1996, after receiving a bachelor's degree in Latin literature and mathematics from Amherst College, and a Ph.D. in computer science from the University of California at Berkeley, is also author of cryptographic thriller "Tetraktys."