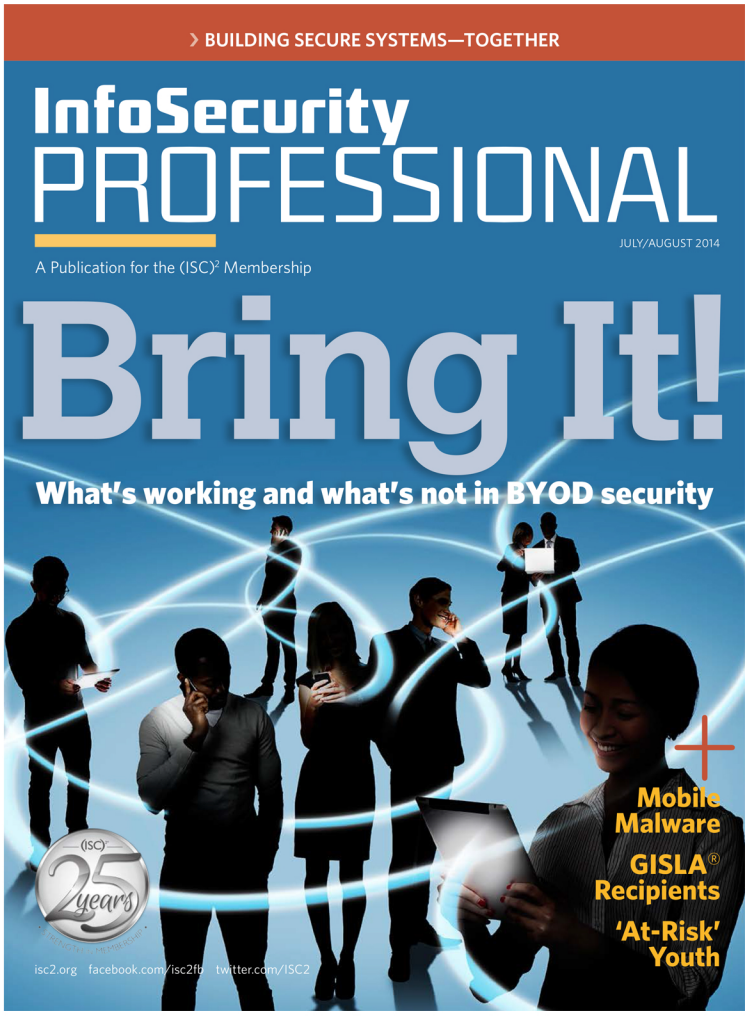
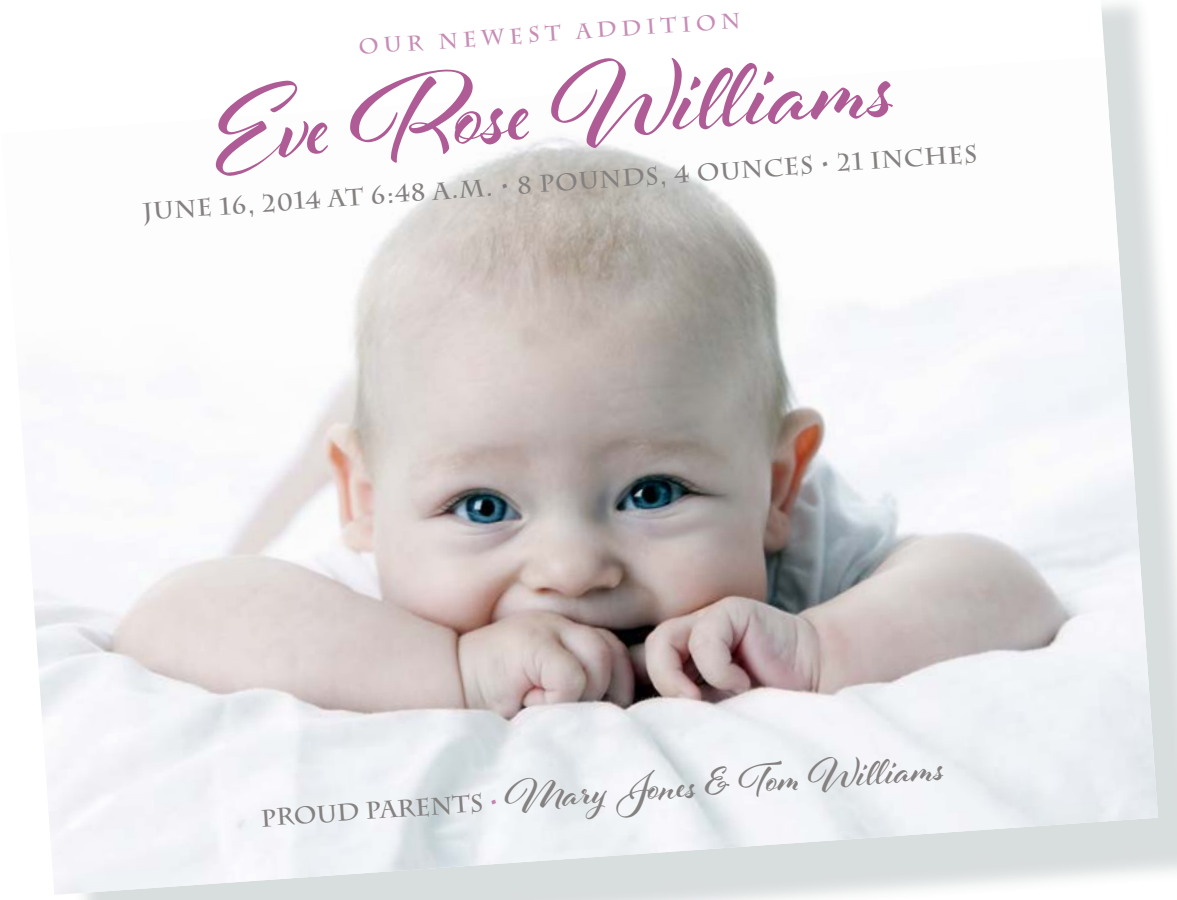


This article was originally published in INFOSECURITY PROFESSIONAL Magazine July/August 2014 issue and is republished here with the express written permission of ISC2

WATCH AND SEE



A CYBER CIVIL RIGHTS ADVOCATE SHOWS HOW WE'VE CREATED A GENERATION OF AT-RISK YOUTH

BY **RAJ GOEL**

TECHNOLOGY HAS ALWAYS existed at the intersection of hope and fear. At the dawn of the Internet age, we dreamt of a world without borders or boundaries for information routed around censorship. Several decades later, we now live in a world that closely resembles the United States television series "Person of Interest," in which we are constantly under surveillance by governments, corporations, law enforcement, our neighbors, and even our family members.

Not only does this erode our expectations (and rights!) to a certain level of privacy, but the vast amounts of data gathered in the course of such omnipresent surveillance also puts us at a much higher risk of fraud and identity theft.

But some of the outrage needs to be directed inward as we, the consumers, continue to aid and abet cybercriminals through personal data paraded on social media and handily offered to mobile apps, just to name two popular practices.

So what about a child born in 2014, who enters this world without much to trace? What information do we need to conduct ID theft or potentially ruin their reputations before they've even said their first word?

Not much.

RETURN TO CONTENTS

WAYS PARENTS AND FAMILY MEMBERS GIVE UP THE GOODS

At a minimum, we need five identifiers to impersonate someone else online or over the phone:

- Mother's maiden name
- Date of birth
- City of birth
- Name
- Phone

Long before a child is born, his parents may have married and announced their nuptials a number of ways, from a formal wedding announcement in the local newspaper (with an accompanying website) to an online site that advertises an engaged couple's wedding plans, including the couple's full names, date of the marriage and location of the wedding. This is how we acquire a mother's maiden name, provided she changed it after getting married; it is not uncommon now in many countries for women to retain their maiden names for personal or professional reasons.

More and more, prospective parents are sharing "Save the Date" or "We're Expecting" announcements. This does not give us a date of birth, but an ID thief now knows around what time to monitor a feed or local newspaper for the official announcement of the arrival. And, of course, social media plays its part by having both major and minor life events (from engagements and births to posts about how a couple first met) advertised on Facebook, Google+, and other sites where stricter privacy settings are often ignored.

As soon as the baby is born, you can expect proud parents or grandparents to send out the "Welcome our Little One" cards, posts, tweets, etc. And even in the age of HIPAA, hospitals across the United States and other nations proudly share the newborn's name, date of birth, parents' names, and in some cases, names of siblings and health care practitioners involved in the delivery.

This is how we acquire the child's full name and city of birth.

Finding a household's phone number that the child eventually "inherits" is just a Google search away, thanks to the many "people finder" services that search engine algorithms seem to love.

HOME IS WHERE THE HEART HACK IS

So, is our baby safe in his/her home?

Not really. More and more, parents are turning to technology to help manage their baby's care. And most consumer-grade equipment was never designed with security in mind.

Just ask Heather and Adam Schreck of Cincinnati, Ohio, U.S.A., who were woken at midnight to a man shouting, "Wake up, baby! Wake up!" in their 10-month-old daughter's room.

Adam ran to the bedroom and found the shouts coming from a Foscam IP Camera aimed at the crib. The camera turned to face the startled father. "Then it screamed at me," Adam told a local television reporter. "Some bad things, some obscenities. So I unplugged the camera."

Most baby cams, baby monitoring systems, and other consumer devices come with either no passwords, default passwords that are never changed, or vendor-coded back doors that can never be secured.

And not every hacker makes his secret presence obvious by screaming at the occupants.

SCHOOL DAZE

School shootings worldwide have led more communities to implement student monitoring systems at public and private campuses to record who comes and goes from buildings or who approaches students on school grounds. Rarely, if ever, do parents balk at the increased safety measures.

But it's a different story when it comes to technologies like InBloom, a database initiative largely funded by the Bill & Melinda Gates Foundation and built by Rupert Murdoch's News Corp. The technology, which as of last year was adopted in nine states, creates a centralized database where student records, from attendance to disciplinary to special needs, are stored. New York City parents, including the current mayor, expressed outrage upon learning that the data could be sold to private companies.

Civil rights groups took immediate legal action to try and prevent the practice of disseminating student data—a practice that also had been taking place in Colorado, Delaware, Georgia, Illinois, Kentucky, North Carolina, Massachusetts, and Louisiana by the time the New York uproar began.

In April 2014, InBloom announced it would shut down.

WORD OF MOUTH

Marketers know that children and teenagers are a financial goldmine. They are easily influenced by advertising that can lead to lifelong brand loyalty. And they love to tell their friends, providing the kind of peer pressure corporations—and data mining dynasties like Facebook, Google, and Twitter—love. Their choices, and choice words, leave a lasting impression—which some come to regret.

That's one reason more and more (ISC)^2 members are volunteering for the (ISC)^2 Foundation's Safe and Secure Online program. Companies are not necessarily going to do right by our children, so we must teach them how to protect themselves when they use Web services and interact online and across public airwaves.

Because, as we adults all know, the Internet never forgets.

To paraphrase the U.S. Justice system's Miranda rights: Everything you say can and will be used against you, by anybody, now or decades into the future.

THE TRACKERS ARE ORGANIZED

So far, we've seen how we've put our children at risk just by being social, friendly, and even caring. But the child of 2014 will inherit governments that have the ability and perhaps the desire to conduct ubiquitous surveillance that could increasingly endanger privacy rights.

It's not just the NSA-funded programs that capture emails, chats, videos, photos, file transfers, login activity, social media profiles from a variety of entities including Microsoft, Facebook, Skype, Google, PalTalk, AOL, Yahoo, YouTube, Apple, AT&T, Verizon, Sprint, etc.

There are provisions in the United States Electronic Communications Privacy Act of 1985 that allow law enforcement to acquire email older than 180 days as well as certain online data with minimal judicial effort. These efforts were augmented by the post-9/11 U.S. Patriot Act. Civil and privacy rights advocates are continually challenging this latitude on the part of the government, but the children born in 2014 will have to learn to protect themselves.

And it's not just the U.S. federal government; law enforcement agencies in cities and towns across the country are beginning to invest in "StingRay"—a

Ways We Put Our Children at Risk for Fraud/ID Theft

- ✖ Birth announcement in the local newspaper
- ✖ Birth announcement on social media
- ✖ Online "people finders" to pin down addresses, family details
- ✖ Posts on social networks
- ✖ Unsecurred webcams/baby monitors
- ✖ School announcements in local newspaper or websites
- ✖ Parents' blogs
- ✖ School databases used for marketing and research
- ✖ Social media monitoring/ impersonations
- ✖ GPS on mobileware
- ✖ POS technology for target marketing

Image ©Didem Hizar-iStock

RETURN TO CONTENTS

technology that can mimic a cell phone tower, thereby intercepting mobile phone numbers. Warrants are not required because the device is collecting numbers, not actual conversations. And police departments are keeping mum about having the technology.

The car you drive and loan to your child is no longer just a vehicle in a stream of traffic. License plate readers, traffic cameras, and other community video functions are capturing license plate data every minute. That data is collected not only by police agencies, but by data collection firms (for sale) and auto repossession companies.

CELL ME SOMETHING I DIDN'T KNOW

It could be said that the cell phone is the best spying tool ever invented, and as users, we enable it and our children are learning to do it as well. GPS tracks our every move (and our children's). Cell phone logs show who we talk to and for how long. Our kids take pictures and share them with their friends on Instagram. Our phones can record what we say. There are apps, like CrowdPilot, that will broadcast our every word.

The cell phone quickly became part of our lives, and it'll be part of the lives of children in 2014 in ways we never even considered.

WHAT'S THE GAME?

So why are we being spied on, and creating a world constantly under surveillance for the children of 2014?

Some will claim "safety": The advantage of knowing where our children are, avoiding getting lost, keeping track of the bad guys, etc. But for most, it's about money.

Those ubiquitous shopping mall cameras track your every move, and point of sale technology notes your every purchase, whether it's cash, debit or credit. The value to the retailer is immense: by knowing your shopping preferences and those of your children, you can be easily targeted on birthdays, anniversaries, sales of your favorite items…all because of the data you've willingly shared.

Consider this true story from Charles Duhigg's best-seller, *The Power of Habit*: retail giant Target used its proprietary data profiling service to determine that a teenaged customer in New Jersey was pregnant, based primarily on her purchase history. They began to mail her coupons for baby products and other materials for expectant mothers. The young woman's father called the store manager to complain that the mailings were inappropriate because his daughter wasn't pregnant. The store manager apologized profusely, believing the technology had malfunctioned. But a few months later, it was the father who was apologizing. Unbeknownst to him, his daughter was indeed pregnant and later gave birth.

That incident took place several years ago. What are we to make of the technological advances since? Everything poses a threat, from drones hovering over neighborhoods to our neighbors hovering over their own Web cams.

THE WATCHERS ARE EVERYWHERE

In London, our child will be photographed by the largest collection of government surveillance cameras in the world. In Russia, his/her telephone and email metadata content, as well as all Internet Wi-Fi, and social media traffic may be monitored by law enforcement.

Whether our children are at home or abroad, they are being watched—but not in the way a parent would prefer. On every continent, we live under the watchful eyes of governments, corporations, and other private entities. It is up to us as parents, citizens, and information security practitioners to help protect the most vulnerable segment of society: our children.

We cannot always compete technologically, but we can certainly do our part to spread awareness and to speak out, as parents in New York City did, when that technology goes too far and places our children in harm's way.

It's important that each of us, as information security practitioners and private citizens, teach the children and adults in our lives that no privacy rights exist on the Internet—not in Canada, the U.K., Russia, China, or even the international space station.

Welcome to the life of a child in 2014. ●

RAJ GOEL, CISSP, *is a cyber civil rights advocate, author, and speaker who will speak about global surveillance architecture at this year's (ISC)² Security Congress September 29 - October 2 in Atlanta.*