No More Secrets

Life, Online
Ryan McClure
Given 27-Jun-20; Sermon #1551c

Some of you might remember the 1992 movie *Sneakers,* starring Robert Redford, Sidney Poitier, Mary McDonnell, and River Phoenix. The movie was about a group of experts who specialize in testing security systems to prove just how secure they really are.

Robert Redford's character heads up this group of 4 or 5 experts, and as the plot unfolds, he ends up being blackmailed by government agents who want him and his team to steal a top secret black box. Of course, they eventually recover the box and discover that it has the capability to decode encryption systems around the world. Think FBI database, energy grids, even air traffic control.

As they are discovering what the little black box can do, Robert Redford and Mary McDonnell are trying to figure out what the company, Setec Astronomy, is all about. Using Scrabble pieces, they begin rearranging to letters to see if they can spell something else.

Sure enough, as they move the letters into their final places, the phrase "too many secrets" is spelled out in front of them. And so, it would seem that whoever is connected to this shell company and little black box, wants to reduce—even eliminate—the cyber barriers propped up to safeguard data and information everywhere.

In the true spirit of a happy-ending movie, Robert Redford and team eventually find out the agents who hired them do not work for the government, they sneak away (pun intended), and the world is a safer place.

Back to the real world: You might be surprised to find out even when early databases were developed, the risk that someone could hack into the repository to gain access to the data was something the government was concerned about from the very beginning.

Most cyber attacks in the '80s and '90s were things like worms, viruses, denial of service attacks, and straight hacking to actually take control of a computer system.

An interesting example of that is what was eventually dubbed the "Solar Sunrise" event in 1998, when two sixteen-year-olds in California, and their 18 year-old mentor in Israel, hacked into the U.S. Department of Defense's computer systems and gained control of computer systems operated by the government, the military, and the private sector.

Heading into the 21st century, we now have what is called cyber warfare, which according to rand.org, **"Cyber warfare** involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."

That's not all. There are other hackers who have found a more lucrative corner in the hacking profession by targeting personal information like Social Security Numbers, dates of birth, credit card

and bank account information. This type of information can either be used directly to set up fake credit cards, execute fraud, or be sold online to the highest bidder who will most likely do the same thing.

Examples include, but are not limited to, the Target credit card and information breach in December of 2013 and the Equifax breach in May-July of 2017.

Finally, and certainly not the last, is ransomware, which is a type of malware designed to block someone from accessing their own data or threatens to expose their data unless a sum of money is paid. In March, April, May, and June of 2019, Wikipedia documents four different counties and cities that were hit with ransomware. Some had to pay in order to get their systems and data back.

And so, as you can imagine, companies all over the world spend quite a bit of money on protecting the company's data and information and that of their customers. RSAConference.com reported in a June 14, 2019 article that, "In 2019, worldwide spending on information security products and services is estimated to reach over $124 billion."

You would think that with all of that information, everyone would have their information on lock down. But, how good are we as individuals at protecting our data and our information? Spoiler alert: Not so great.

Do you remember that sound of the 56k modem connecting to the internet? It took like 5 minutes to get onto the Internet. Back then, you might have paid monthly for an email address. You surfed the World Wide Web anonymously, hardly logging in to any site; you were to moving around, reading articles and such. Then Google came along, and all of a sudden, things were free. Free email, docs, spreadsheets, chat and more. But was it then, or is it now, really free?

In a March 5, 2012 *Forbes* article, written by Scott Goodson, titled, "If You're not Paying for it, You Become the Product", Goodson finishes the article by saying,

> Which leads me onto my final point - in this digital age we have sacrificed our privacy in order to access all manner of free stuff on the web. It's a movement that most of us have come to accept. Or have we?
>
> I'll borrow a quote I read on MetaFilter recently: 'If you're not paying for it; you are the product'. I'm not sure how many people are fully aware of this sentiment yet or whether they even care. But the next time you're browsing the web or enjoying a video on YouTube, remember that Google is watching your every move; because that's the price you pay.

It's not just Google. As you surf the web, there are these little things called cookies that track your personal information. There are all types of cookies: Session cookies, Permanent cookies, Third-party cookies, Flash cookies, even Zombie cookies. (I'm waiting for them to come out with the Cookie Monster.) This tracking is done to provide a "better browsing experience", to "only provide relevant advertising," to "make your life better," they say.

It does not stop there. Location services, hashtags, photo tagging, and nowadays, the Internet of Things or (IoT). Alexa, Siri, Cortana, Google Assistant, Bixby and more are scattered about our homes. Finally, most of us have our very own personal tracking device right in our pockets each and every day.

It is with that phone (usually), that we take selfies, photos of the kids, the family, dogs, cats, vacations, and more. We post to Facebook and Instagram, maybe tweet or retweet since we just finished posting. Maybe we Like, Love, Hug, or not Like a post because we agree with it, feel sorry for it, or do not really like it at all. Eventually, as the years tick by, picture by picture, post by post, these data sharing companies essentially store our lives, along with pictures, and build our digital profile. More on that in just a bit.

Anonymity, I think, is a thing of the past as it relates to your digital profile. Let me explain. Let's say a new person joins your team. We will call him John Smith. You meet John and are curious about who he is, so you see if he has a LinkedIn account. Sure enough, you find his picture out of the millions of other John Smiths, and you now know his complete education down to the high school he attended.

On to Facebook. You are armed with more than a first and last name, and easily find him along with who he is friends with, what his wife looks like, and some of the vacations he has taken recently. Wow! He drives a nice Mercedes, and look, those must be his two cats that he adores.

You notice that he has liked and loved a lot of Republican or right-leaning posts, articles, and pictures, so you deduce he is conservative. Over to Instagram, and based on the pictures and posts, it looks like he and his wife like to party on the weekends. In fact, every weekend.

You wonder what kind of house he lives in, and so a quick search on Google and maybe even the county tax records, you now have an address. Over to realtor.com, and from the looks of the 5,000 square foot home he and his wife have, they must being doing very well.

Now anyone, armed with a name, the internet, and some patience, can do exactly what I described, and more. If a common person in the street can do that, what do you think the companies that hold all of our personal information can do?

Each one of us, based on the apps we use, the posts we write, the things we like and yes, *even* the things we don't click or don't like—all of it is used to build our online digital profile, and it is being captured and stored and someday might be used against us. One needs to look no further than the social credit system employed by the Chinese government to see how it could all come together.

Honestly, look at the stars, business people, even everyday people that recently have been subjected to sudden, immediate, and even instantaneous termination from their jobs because they liked a tweet or post that goes against mainstream thinking.

In the September 10, 2018 Forbes.com article titled, "What Does It Mean To Live Our Entire Lives Under Digital Surveillance?" commentator Kalev Leetaru states, "A child of the digital era will have their life broadcast to the world from their first ultrasound to the day they die." Later on in the article, he states,

> Perhaps the most frightening element of this dystopian reality television world is that the social media and other platforms into which all of this data is being deposited are not merely passive content hosts. Rather, they are actively mining and profiling their users, building enormously rich and ever-more detailed dossiers that can not only predict everything from an individual's sexual orientation to their political leanings, but make all of that information available to advertisers, data brokers and myriad other companies to buy and sell at will.
>
> What happens to the adolescent who is just beginning to discover their voice and unique independent personality when they stumble onto Facebook's advertising categories for their account that have precisely pinpointed every possible attribute of their existence, from their beliefs and interests to their sexual orientation?
>
> Will they be aghast at the privacy violation or treat the experience like algorithmic fate charting out their entire future?

We know as we read in Luke 8:16-17,

> **Luke 8:16-17** For nothing is secret that will not be revealed, nor anything hidden that will not be known and come to light.

We also see in Hebrews 4:13,

> **Hebrews 4:13** And there is no creature hidden from His sight, but all things are naked and open to the eyes of Him to whom we must give account.

God does indeed know everything about us; we are not hidden from Him. That transparency is a good thing, because God is working to shape us into His image.

But what is the upside for us that these companies have all of our data, our personal information? Could we be penalized for something posted, tweeted, liked, even not liked? We are certainly free to say and do what we like, but is free speech really free, or does it eventually come at a price?