Chapter 4
The Era of Homo Digitus

Evelyn de Souza

We have emerged as a new species. We have become digital beings whose lives are closely anchored to digital objects: Deep learning, artificial intelligence, and behavioral analytics are no longer buzz words; they are part of our new reality. From a security and privacy perspective, there are new and different considerations. That's why it's fitting to focus on the concept of Homo Digitus, which I first learned about in "*The creative destruction of medicine: How the digital revolution will create better health care,*" by Eric Topol, and more recently highlighted as a Gigaom conference theme.

This chapter expands on a concept I wrote about in CloudTweaks last year In Topol's vision there is a new human species, *Homo Digitus* that benefits from the data deluge brought about by the convergence of the digital and physical world. They track sleep quality with brain-wave headbands, monitor vital signs with wrist transceivers and use cell phones for self-diagnosis amongst other things, realizing the opportunity for a much more evolved life.

In this chapter I will focus on the following from a security and privacy perspective:

- Technology Transformation for Homo Digitus
- Safeguarding Data, the Lifeblood of Homo Digitus in the Enterprise
- Gender Evolution in the Era of Homo Digitus

E. de Souza (✉)

D.A. Christofferson (ed.), *Women in Security*, Women in Engineering and Science, https://doi.org/10.1007/978-3-319-57795-1_4

Technology Transformation for Homo Digitus

Each evolution of the human species delivers on the promise of a smarter human far more capable than the species that preceded it. In earlier species humankind looked for new ways to improve hunting and gathering of food and in some parts of the world, such was their mastery that they even created an oversupply of certain foods.

Homo Digitus sees data as the new food and you'd be challenged to find any facet of life that has not been revolutionized by data deluge—there are a great many varying estimates, on how much data is created every year but everywhere you look volumes of data are soaring.

Mostly, it's been for the better good of humankind. Hands-free control of technology improves the lives of people with physical disabilities, makes healthcare and other professional services more efficient through accurate voice dictation, enhances automobile safety, and makes everyday tasks more convenient.

With new data points, we've also experienced great transformation in the quality of services and business process too. We've come to have a great reliance on the benefits that data deluge brings. If you consider how often an individual might use map services to estimate a commute, or an app to compare shopping prices, and then for business the productivity and economic gains from using data points to estimate customer preferences, improve customer service and speed business delivery times.

Will Your Internet of Things Device Testify?

However, a strong note of caution and a real-life scenario: Your wearable device is subpoenaed to testify against you. You were driving when you were over the legal alcohol limit and data from a smart breathalyzer device is used against you. Some might argue that such a use case could potentially safeguard society. However, it poses a bigger concern about how data from the broader spectrum of connected devices or apps could be used against you.

Doesn't it seem reminiscent of George Orwell's dystopian universe, "*Nineteen Eighty-Four*" where children were indoctrinated to inform on suspicious activity, only now it's a connected device? But, this time it's you who chose to use the device or network of devices, or apps that could start working in concert against you.

Some might see this as the gradual erosion of privacy, but in the era of Homo Digitus, privacy will be redefined. There won't be a universal single definition; each person will have their own privacy threshold about the level of data they feel comfortable sharing with third parties and about the implications of that for their futures.

Controlling Data Deluge to Maximize on Homo Digitus

One of the downsides of the era of Homo Digitus, is that data has been exploited and misused in ways that leaves humankind fragile and that puts businesses at great risk. Data breaches, privacy infringements, identity and data theft abound**.**

When new technologies are released that introduce microphones or other recording devices for the first time, or seek to use data in new ways, companies need to provide additional transparency and greater levels of control and choice, and in a way that consumers can readily digest. In particular, we need to look out for older people who technology might be anathema to and children (see further on) who may run the risk of being exposed or harmed in ways unintended.

Until these standards are in place, I encourage users to be vigilant and to press manufacturers for clear answers on the following at minimum:

- **Will your data be shared with third parties?** This is particularly important for any device that collects sensitive data about you. It may be challenging given the volume and legalese of privacy policies but well worth the time investment given it's your private data.
- **Understand how your information is transmitted.** And, once in storage, who has access to the information? Is the information stored on a third party's cloud? When you stop using the device, what happens to your data?
- **Take time to understand your device's privacy settings**. Have you configured the device's settings maximum privacy? Are you only sharing what you are comfortable sharing publicly?

Protecting Our Next Generation

Unlike in the physical world, danger is far more difficult to discern. In the physical playground, an object hurtling in the direction of a child might be the cue for a child to move away. Whereas in the digital world events that may result in financial harm of personal exposure may occur stealthily over time or suddenly without warning. Parents tend to be more watchful of their children in a physical playground and teachers watch over children during recess and lunchtime. While many parents are very diligent and keep a steady watch over their children when they are on online, it can be challenging to monitor everything a child does online given its pervasiveness.

When children use computers, tablets or mobile devices, they may think that their information is stored somewhere on the device. And, as savvy as they may be with navigating their way around a device, they may not always realize that their data has been silently and without any cue transmitted to cloud storage.

The good news is that in many parts of the world, privacy laws are catching up with many cloud-based applications. Regulations are increasingly requiring parental consent for collecting certain types of sensitive data and prohibiting the use of children's data for marketing purposes. Regulators are also cracking down on deceptive practices, especially as they pertain to children and those who may be vulnerable.

However, until we have consistent regulations and standards, parents, adults and teachers need to exercise even greater caution and oversight as compared to the outdoor playground. It's the reason why online safety classes needs to be a standard part of all children's education today. And, it's the reason why I am focused on accelerating digital safety initiatives, not just for business usage, but for everyday living also and especially for a safer playground for our children, especially my niece and nephews.

Safeguarding Data, the Lifeblood of Homo Digitus in the Enterprise

What's needed is a way that allows Homo Digitus to benefit from the positive effects of data deluge but with the safety net that data flows are being directed to only those authorized to have access.

In the workplace, digitization has changed how we work—it goes beyond the devices we use and where and when we work, and more to the tools and data and our interactions with an expanding network of people and data. Yet, despite the fear around security breaches, there are few security approaches that truly focus on securing at the data layer with a contextual focus on people and the expanding number of applications in use today.

In an enterprise being able to proactively determine data flows and then implement additional safeguards based on a comprehensive set attributes ranging from geolocation, network, and device down to multiple facets of identity will be critical, given the sophistication of data exploitation.

Information security tools have traditionally been associated with impeding progress. Newer solutions need to be easy to implement and policy attributes stated in a way which are business-consumable, so that business leaders standing up new services can easily understand security and privacy implications versus having to navigate security speak.

However, as great a risk might be posed to businesses from well-intentioned individuals, who might accidentally misuse or overshare data. It's only natural considering that for many individuals digitization occurred midway during their lifespan and dealing with the data deluge is not yet a completely natural phenomenon. Also, our lives are increasingly fast paced, workplaces are more pressurized and the convergence between home and work narrower, that workers are prone to accidentally misusing data.

For example, it's very easy to accidentally drag and drop a file into an email and send as an attachment. Toolsets that can alert users to a potential data misuse can greatly alleviate this situation while allowing users to perform their work duties in an efficient way.

Cloud and Data Multiplication

Cloud computing has become the term du jour in the industry and its evolution has enabled highly scalable and elastic services via the Internet and cloud has become the back end for so many aspects of our daily and work lives. Organizations leveraging cloud services to store this data may need to take a closer look at the lifespan of the data they collect and how it is expired and destroyed.

Today's organizations need to understand that cloud as a model causes data to multiply further. The dynamic nature of resource allocation and maximizing availability in a hybrid or public cloud means resources are replicated and backed up across multiple data centers. While there isn't a universal blueprint for protecting sensitive or mission-critical data, the following is a good starting point.

- **Tag all sources of mission-critical data:** It starts with strong preventative measures: If data is classified digitally to a scheme that is intuitive to your cloud provider and your organization it will be easier to track through its lifecycle and then expire and destroy.
- **Take time to assign entitlements and access rights:** Ensure that access rights or entitlements for sensitive or mission-critical data are limited to only those who have a legitimate need for access.
- **Apply encryption based on context:** When data is encrypted, it is only readable to those with access to the encryption keys. It is the most certain way to limit unauthorized access to data in the cloud. By encrypting organizations can be better assured of the confidentiality of their data and potentially be less concerned with their cloud providers' data destruction methods.
- **Perform data wipes:** Many government and industry standards require data storage wipes to ensure that hardware is safe for reuse. There are different types of software and hardware that even allow for remote erasure. The benefit is to enable a provider or enterprise to repurpose the media for reuse.
- **Physically destroy data and media:** In the cases of highly classified information organizations can use strong magnets to destroy data or even shred physical media. This ensures that the data on the destroyed media can never be recovered. Physical destruction methods are the last resort and only feasible in a private cloud environment.

Gender Evolution in the Era of Homo Digitus

Though the industry has seen the rise of this and other great technological revolutions, the gender evolution is moving much more slowly. Bridging the gender gap matters.

How can solutions for our future be architected primarily based on the input of the XY chromosome and without input from the XX chromosome? It's the Yin without the Yang. While there are some impressive female role models today in the digital industry, having women in more balanced numbers across engineering and product functions will lead to more innovative and functional solutions. Research suggests that stronger links between left and right hemispheres in women makes them better at intuitive thinking and demonstrating flexible attitudes.

As you embrace digital living, be sure to think about ways you can help bridge the gender divide:

- Encourage girls and women who are interested in technology to seek the support of organizations who mentor and nurture girls and women in technology
- Attend girls and women's' technology events to demonstrate your support for stronger gender balance
- Find ways to attract women as you look to hire for engineering and product development roles
- A key finding from a recent study "Addressing Gender Gaps in Teens Cybersecurity and Self Efficacy" was that teen girls were likely to develop confidence and interest in cybersecurity through informal approaches. It's a great opportunity for cybersecurity practitioners to become role models and mentors to a younger generation. I noted earlier that many cybersecurity approaches lag as much as 10 years behind the business landscape. Overhauling industry approaches is difficult when approaches and toolsets have been in use for decades. That's where reverse mentoring can play a role. Partnering with young people is not just about them learning from us; it's about what we can learn from them.

Homo Digitus is still in the process of being shaped. Now is the time to ensure that data deluge remains the positive enabler. With each evolution of living our lives have become much more strategic and filled with interesting possibilities compared to previous generations who may not have had as much choice as we have. It's time to drop the fear-based messaging. That would help us focus on technology as an enabler and to address issues that are gray or unclear versus fear-mongering which often serves to hold people back.