Chapter 3
Cybersecurity and Privacy in the Age of the Pandemic

Anastasios Arampatzis
Independent Researcher, Greece

Louise O'Hagan
Queens University Belfast, UK

ABSTRACT

The unprecedented acceleration of digital transformation in response to the pandemic migrated businesses and people to the always connected world of the internet. The reliance on digital technologies introduced novel cyber threats that increasingly targeted the human factor. As people had to face technology-mediated information overload, navigate health concerns and anxiety regarding the virus, and balance life and work in their hybrid offices, arguably cybersecurity and privacy concerns may have been overlooked.

INTRODUCTION: THE WINDS OF CHANGE

The United Nations (2020) characterized the COVID-19 pandemic as one of the most disruptive events faced by humanity. By mid-2021, the United States marked half a million COVID-19 deaths and countless infections. In addition, the global economy suffered severe impacts and uncertainties.

Effects of COVID-19 migrated from the physical to the virtual world as we relied more heavily on the internet and adapted to a digital economy. Systemic issues that had previously been hidden behind the perceived benefits of the internet began to surface, including: the ability of digital infrastructures to sustain increased pressures; lack of access to digital services by poor or marginalized populations; and increased dependencies on complex supply chains (World Economic Forum, 2020). In fact, the virus only highlighted many issues and risks that existed pre-pandemic.

Throughout the pandemic, individuals would rely on technology and digital platforms as they moved more online to complete personal, essential, and professional activities. These online activities create both personal and behavioral electronic data. Personal data identifies the owner of the data. Examples include names, dates of birth, locations, log-in details, postal addresses, social security numbers, genetic

DOI: 10.4018/978-1-7998-8630-3.ch003

data, curriculum vitae, internet protocol addresses (IP address), gender, birth certificates, reference letters, phone numbers, nationality, health records, passport information, financial account information, driver's license numbers, health details, and biometric marker information (Solove & Citron, 2018). This type of data tends to be factual and permanent. For example, a person cannot change their date of birth and rarely change their name.

Behavioral data is created by Internet users' online activities. This type of electronic data is created through online services and platforms like online shopping, fitness tracker apps, Web searches, and other types of engagement via an Internet-connected device. Behavioral data tracks and collects location information, including location of the device, an app downloaded on the device, and the device network provider. Location information can be associated with behavioral events. For example, if a phone location is a COVID-19 test center, it can be presumed that the person is getting a COVID-19 test.

Another type of behavioral data is health data, which is created and collected from wearable computing devices (i.e., pedometers, smartwatches, head-mounted devices) that measure number of steps per day, cycling routes, and heartbeat. These types of data can tell what is going on in users' real-time movements (Dong, Lepri, & Pentland, 2011).

Users are not fully aware of the collection of behavioral data. Often, the user has given consent to the collection and use of their behavior data by agreeing to a website's or app's terms of use and/or policies.

Both personal and behavioral data are "user-generated," resulting in the creation of increasing amounts of exploitable data and placing an individual's privacy at risk. It is nearly impossible for humans to avoid producing digital user-generated data. Electronic data holds monetary value when collected, stored, and analyzed; therefore, corporations and criminals sell this kind of data with the goal of financial gain (Charitsis, Zwick, & Bradshaw, 2018).

The growth of technology use and value of data means that monitoring through online services ("surveillance capitalism") is becoming increasingly common (Zuboff, 2015). According to Zuboff (2015), surveillance capitalism exists because user-generated behavioral data introduces new prospects through observation and estimation, which leads to the alteration of human behavior. The pandemic's increased reliance on technology created even more surveillance. This observation of patterns and trends in user-generated data creates a new reality. This shapes our lives and targets consumers via personalized ads.

Most users are unaware of the extent to which their movements and behaviors are captured and observed. They are also typically unaware of how the use of this data will modify their lives (Mamaeva & Mamaeva, 2018). It increasingly encroaches through unexpected domains. For example, electronic data has taken a dominant role in modern politics, advertising, our daily public lives (van der Velden & Milan, 2018). Availability of the pandemic's extra user-generated data has created opportunities for exploitation by criminals and corporations. Some new industries have developed online platforms and analytical tools to understand behavior patterns in the data, predict future behaviors, and persuade users (Gray, 2018). The data is analyzed, processed, and used to make decisions with real-life consequences on users.

Businesses across the globe were ruined. According to the World Economic Forum (2020), the pandemic created a unique crisis, causing turbulence in the global economy, disrupting global supply chains, and transforming society. To ensure their existence, businesses had to adapt to the new reality. As a result, businesses accelerated their digital transformation initiatives. Businesses migrated to the cloud to support work from home and/or remote work that impacted employee and customer access to corporate data and services. Cloud deployments allowed organizations to reap the benefits of flexibility and scalability, increase productivity, and reduce operational costs.