CHAPTER 5

Big Data as a Creeping Crisis

Swapnil Vashishtha and Mark Rhinard

Abstract This chapter examines the mass accumulation of private data in terms of a creeping crisis. The threat at hand—commonly referred to as "Big Data"—pertains to the direct compromising of personal integrity and safety. The chapter explores the driving forces behind this threat, identifies the precursor events or "flare-ups" of the deeper problem, and documents the varying levels of scientific, political, and public attention given to the problem. Our analysis reveals the breadth of the problem and the main challenge to managing it: societies' deep dependence on the underlying technologies and systems. Addressing this creeping crisis will require substantial government intervention to regulate privacy and effective horizon scanning to track its many possible costs.

Keywords Creeping crisis • Big Data • Data breach • Privacy • Data accumulation • Cyber security

S. Vashishtha (✉)
Swedish Institute of International Affairs, Stockholm, Sweden
e-mail: swapnil.vashishtha@ui.se

M. Rhinard
Swedish Institute of International Affairs, Stockholm, Sweden

Stockholm University, Stockholm, Sweden
e-mail: mark.rhinard@ekohist.su.se

A. Boin et al. (eds.), *Understanding the Creeping Crisis*,
https://doi.org/10.1007/978-3-030-70692-0_5

5.1 Introduction

With increasing frequency, experts warn about the accumulation of "Big Data." Some scholars call the exponential growth, storage, and manipulation of individuals' most intimate details in the hands of private actors a wicked policy problem (Gruetzemacher, 2018; O'Neill, 2016). Others refer to an impending crisis (Krebs, 2016) or to the intractable vulnerability of modern society (Zuboff, 2020).

The phenomenon of Big Data took root decades ago. Technological advances combined with widespread use of the Internet to create a new threat. Early warnings by lone experts and individual politicians, in the 1990s, were cast aside as scaremongering. As the problem grew, attention grew—but only sporadically. The scale of the problem expanded from one of moral concern (losing control over one's own identity) to financial vulnerability (undermining one's economic stability) to a geopolitical issue (opening new vectors for attack). Actual events outlined below drew periodic outrage, following revelations about the size of the problem (e.g. the Snowden incident), the ease at which data can be stolen (e.g. regular data breaches), and how data can be used as a weapon (e.g. accusations made against Russia and China). Few politicians today dispute the underlying problem and the potential for a much larger crisis ahead. Some regulatory action has been taken. But sustained attention, and any comprehensive management of the issue, is hard to come by. According to some, we are "standing on the edge of a precipice" (Buck, 2011).

Big Data thus reflects the archetypal creeping crisis defined in the introduction to this book. It emerged incrementally over time, accelerated because of interacting developments, reveals itself through precursor events, and fails to sustain political attention or proper crisis management. What this chapter showcases about Big Data, as a creeping crisis, is twofold: (a) the evolution of the problem over time, in such a way as to "creep" into societies' basic functioning without widespread notice; and, (b) how our dependence on the conditions that enable Big Data prevents a concerted response. The chapter highlights the question of how much recognized damage capacity is "enough" to prompt a response, and suggests we may be doomed to live with some creeping crises.

To illustrate these points, the chapter begins by outlining what is at stake: by what measure can Big Data be described, objectively or subjectively, as a threat? We then show its origin and serendipitous emergence over time, before tracking public attention to the problem. Attention is linked to a number of precursor events that revealed the depth of the creeping crisis. We conclude by discussing what has been done, what needs to be done, and why a comprehensive response is likely to be difficult.

5.2 Defining the Threat: What Is at Stake?

With every click of a mouse, every field entered in a website, every query on a search engine, and every application for a loan or job, companies and governments collect enormous amounts of our personal information. We hand over this information both voluntarily and involuntarily. Even where voluntary, banks and governments take our personal details as a condition of service. It is not optional. From those mountains of personal information, it is now simple to deduce where we walk, the way we vote, how we travel, what we buy, our illnesses and maladies, and even to predict our next moves; whether we plan on divorcing, getting pregnant, or switching political parties—even before our closest loved ones know it (Duhigg, 2012). We no longer hold sovereignty over our most intimate and personal information.

The collection of citizens' information is a long tradition, dating back almost a century. Similarly, the digital storage of information is nothing new (Hacking, 2015). The difference today is three-fold. First, the amount of data that can be collected has skyrocketed. Census taking in the 1700s collected information through personal interviews and was hand-written into obscure logbooks. Today, thousands of "data bits" about our personal circumstances are transferred every hour, owing to technological developments, efficiency goals, and profit motives. Second, the processing of that data has grown more sophisticated. Data that once stood in dusty folders, or rarely examined databases, is now recombined with thousands of other data points, and run through algorithms, to produce our profiles and to deduce our behavior. Third, these results are now commoditized. Governments—such as police departments—have quickly come to understand how data-driven analysis can promote policy change. Companies sell this data, without individuals' consent, to other companies for vast amounts of money. Companies like Google, Microsoft, and Facebook now derive most of their profits not from services, but from selling our data to secondary markets. This has been called the third industrial revolution (Zuboff, 2019).

The vast accumulation of personal data plays into the hands of those who wish us harm. Such harms range from irritating to deadly. Private firms' use of mass data to shape our behavior and form opinions of us can lead to failed job applications and rejected insurance claims. Rogue agents in our own governments can exploit private data—illegally—to track suspected criminals or profile future suspects. And foreign governments can hack the data on an entire population to attack societal weak spots, blackmail leaders, or shut down health systems. More broadly, the surreptitious collection and use of data undermines individuals' sense of control and personal privacy (O'Neill, 2016). Trust in government—already at risk in an era of creeping crises—could decline as citizens question why their leaders failed to act.

Citizens and experts express concern. A long list of precursor events signals the deeper problem of Big Data and has led to protests and outrage: The shock following Edward Snowden's revelations of how the US government used private data to spy on households; The public anger after the illegal manipulation of Facebook by Russian agencies to target key constituencies during the 2016 US Presidential election; Outrage—and lawsuits—following high-profile hacks on Equifax, Target, and Sony (after which private data was sold to criminal networks); And the forced resignation of ministers in Sweden following the improper handling of private data in the field of transportation. Experts warn that the next step could be catastrophic: a hostile attack on Western society based on the illegal mining of insights from Big Data. How did we end up here?

5.3 Origin and Development

The *origins* of Big Data span back to the 1970s, when micro-processing advances and an obsession with technological efficiency combined with the widespread adoption of the personal computer. Early data-processing machines were built to speed numerical tabulations (Ceruzzi, 2010) and by the 1970s and 1980s, the race was on to shrink their core components. Simultaneously, engineers envisioned shrinking the core part of the internal calculation machinery: the microprocessor. The advent of microprocessors was nothing less than a revolution (Abbate, 1999). By the 1980s, tiny—yet increasingly powerful—microprocessors were making their way into consumer products such as cameras and automobiles.

The rise of micro processing intersected with the advent of personal computing. The first micro-computer using advances in micro processing was introduced in 1975—the Altair 8800 (Mims, 1985). Computer advances remained within the realm of hobbyists and industrialists until

IBM introduced its new, user-friendly, and affordable PC in the 1980s with the help of Microsoft and its software. Shifting from highly technical, confusing systems with limited functions to a system in which software allowed the average individual to operate it, IBM created the PC for the consumer market (Bride, 2011). The rise of the personal computer symbolized a new era in the digitalization of the human experience. But that was just the start.

The accelerating *development* of this creeping crisis—the transition between gradual development and sudden escalation—occurred because of several interacting, enabling conditions (for a summary of these, see Fig. 5.1).

One condition was the development of the Web 2.0 during the 1990s, characterized by a shift from static web pages to interactive, user-generated content. This shift offered a more user-friendly and interactive platform for use of the web, which could be used by a wider range of the population (O'Reilly, 2007). In turn, this enabled a move away from desktop-based software toward "cloud computing," which further spread the reach of software and applications. Cloud computing multiplied the computing power available to individuals and propelled the movement of everyday tasks—from banking to communicating to shopping—to the Internet. At the same time, it represented a dramatically more efficient way to generate, collect, and store data (Wolcott, 2008).

Another condition was the ubiquitous use of smart phones. The rise of smart phones combined with the advent of Web 2.0, since the latter was compatible on every kind of device. It also served to shift most telephony functions (e.g. text messaging) onto the web. While IBM's "Simon" personal device was officially the first smart phone, Apple's initial Iphone in 2007 marked a key point in history, after which smart phones became virtually ubiquitous (Andrew, 2018). The proliferation of smart phones

Initial conditions	Interacting conditions	Result
• Advances in micro processing	• Web 2.0	• Data accumulation
• Rise of personal computing	• Smart phones	• Data manipulation opportunities
	• Social media	
	• Web commerce	

Fig. 5.1 Initial and interacting conditions that propelled a creeping crisis

put the Web 2.0 in everyone's pockets, which allowed the average individual to use new kinds of applications (maps, videos, social media), thereby generating more data and allowing this data to be collected and stored. The transfer from data from private citizens to third parties moved from a trickle to a rush.

Social media further intensified developments. The apparent convenience of interacting with friends and staying in touch with family and colleagues was based on the principle of data sharing. MySpace, Reddit, Twitter, Facebook, WhatsApp all provided a platform for individuals to interact and share information, essentially turning private information public. Many of these, but not all, rose with the rise in smart phones, the convenience they offered and became more popular as more individuals joined (Ortiz-Ospina, 2019). These programs accumulated large amounts of unstructured data. In other words, the data generated can be put together to learn about one's likes, dislikes, preferences, opinions and movements; which in turn can be used to create a personality profile.

Another facilitating condition emerged from the economic value found in personality profiles: the rise of e-commerce. E-commerce was introduced in the 1990s, with platforms such as Amazon and eBay emerging long before smart phones and social media were introduced and became widely popular (DePillis & Sherman, 2018). However, with the introduction of social media and smart phones, e-commerce firms realized a massive change in how they could use the data being generated from social media and smart phones to target consumers with relevant advertising (Erevelles, Fukawa, & Swayne, 2016). Marketing strategies changed as more and more data became more easily available to third parties such as Amazon, who could not only use data generated and collected from their own platform but also from other platforms such as Facebook.

These various conditions interacted with one another to further the facilitation of data generation, collection, storage and interpretation—the foundation of Big Data.

The development of Big Data into a threat represents a kind of tipping point, arrived at after a long trajectory in seemingly distinct systems and shaped by multiple trends. While linear in most respects, this development jumped tracks as new technologies became available. Big Data, as other crises in this book, remained unnoticed by large swathes of the population. Lack of attention amongst some "experts" might have an origin in self-interest. To blow the whistle on Big Data is to call into question the current tenets of the modern, globalized economy and those who profit from it. Certainly, there is a problem of ownership (Boin & Lodge, 2019): no single actor in any government was responsible for responding—and powerful interests would no doubt resist such action. Consistent with the classic crisis incubation thesis (Perrow, 1984), Big Data "crept" onto the crisis scene rather quietly.

5.4 Emergence of the Threat

The interacting conditions discussed above gave rise to the threat agent behind this creeping crisis: the accumulation of data at a pace the world has never before seen. According to Hackenberger (2019, p. 291) "the world is currently creating as much data in two days as humankind has created in the previous 2000 years." That data is largely (but not completely) private in nature and is attached to individuals' personal characteristics. Whereas data was once collected and stored in highly "structured" formats—meaning, for a limited purpose and with few ulterior uses—data today is highly unstructured. It is sucked into enormous databases alongside huge amounts of other data, recombined into new forms of data, and used to find "hidden meaning" (Grable & Lyons, 2018).

This process of gathering data and analyzing the hidden meanings behind the presented data is called data mining and has spawned an entire profession of "data scientists" (Erevelles et al., 2016). Mining is done by insurance companies, banks, casinos, governments, and retail sellers of every kind to help analyze and find patterns out of vast amounts of data—as well as to predict future behavioral patterns. Much of this has ostensibly positive uses—to improve customer services, to customize search results, to reengineer products, to predict customer needs, and to generally make life more efficient. Ford's driver-command systems can be improved and customized centrally, through data aggregation that allows profiling of the customer's most intimate behaviors (Erevelles et al., 2016). Ford uses special software, such as sensors and remote app-management tools, to analyze the data being gathered. Similarly, Google can use Google Maps to assess whether or not a consumer actually visits a physical retail store after visiting the website online (Erevelles et al., 2016).

The threat agent behind this creeping crisis threatens core societal values concerning personal integrity, control, and privacy, along with the effective functioning of life-giving systems. The foreshadowing events, which we turn to below, reveal what is at threat, concretely demonstrating physical harm (e.g. private data theft leading to stalking), financial harm (e.g. identity theft to access bank accounts), and emotional harm (e.g. loss of privacy and individual liberties). Many experts argue that these events are just the tip of the iceberg: that more dangerous situations loom beneath these examples, waiting to be exploited. Such situations will not only harm individuals, but also destabilize society more generally.

5.5 Foreshadowing Events and Attention

Like a campfire casting sparks, creeping crises throw out foreshadowing events. Attention focuses on extinguishing those sparks while the central fire burns on. The analogy of "flare-ups" works in the case of Big Data, too.

For Big Data, precursor events occur with increasing frequency (see Fig. 5.2). By studying a subset of these events—Snowden revelations (2013), the Target Data Breach (2013), the Sony Studios Data Hack (2014), The Yahoo Data Breach (2016), the Cambridge Analytica Scandal (2016), the WannaCry Ransomware Attack (2017), the Equifax Data Breach (2017), and the Marriott Data Breach (2018)—we see common patterns in how these individual manifestations of the broader creeping crisis arose, were acted upon (or not), and then retreated from public attention.

Most of these events were made possible because of the massive accumulation of personal data today. Each was preceded by expert warnings of impending danger, specific either to the event or in abstract. And each involved leaders ignoring warning signs. For instance, each was preceded by security alerts, either by whistleblowers or by tenacious journalists. There were investigations revealing that executives of these firms were aware of deficient security systems and even chose to hide dangerous breaches that compromised individuals' privacy and safety.

Considerable foot dragging surrounds these events. In 2015, the chairman of Marriott corporation was notified of malicious malware embedded in the IT systems of Starwood, which Marriott was on the eve of acquiring. Yet the problem was ignored, and the sale went through

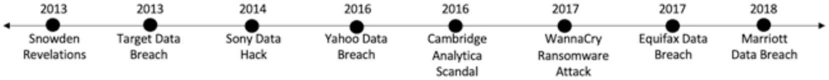

Fig. 5.2 Foreshadowing events

(Shepardson, 2019). Equifax in 2017 was made aware, two months before it became public, of foreign hackers in their systems. Little was done to prevent the massive data theft that took place soon thereafter (Newman, 2017).

Many companies and governments failed to conduct simply upgrades—"security patches"—to close loopholes and prevent easy breaches (Microsoft, 2017). A massive breach of the UK's National Health System (NHS) was made possible by a delayed upgrade (National Audit Office, 2018). In 2015, Mark Zuckerberg failed to formally file complaints against Cambridge Analytica, who had data on Facebook users it was not supposed to have (Kozlowska, 2018). Hoping to avoid a scandal, Facebook merely asked Cambridge Analytica to delete the data—which never happened. In 2013 and again in 2014, Sony received warnings about a likely hack, which executives ignored until the break-in took place (Szoldra, 2016). Target faced a similar situation in 2013 when an intrusion had already occurred in their system, but it went unnoticed (Zetter, 2014).

Sporadic, expert attention gave way to major public attention after each incident. Governments came to realize that the magnitude and nature of these hacks were not confined to companies (even if these companies held immense amounts of public data) but also included threats to national security. Governments in various parts of the world (North America, Europe, and Asia included) became particularly engaged with the national security implications became clear—such as when China was implicated in the Equifax case. There was a huge public uproar surrounding the Cambridge Analytica incident, leading to boycotts of Facebook and calls for greater regulation (Lang, 2018). A typical refusal of responsibility can be found in Target's data breach in 2013, when Target executives failed to acknowledge their role in protecting consumer credit card data. Meanwhile, the blame was also put on credit card companies for not having up-to-date cards with EMV technology, widespread in Europe but not in the USA, which prevents the re-sale of stolen card information from Target's systems (Zetter, 2014). Lawmakers were also blamed for poor regulations—including weak security standards for corporations and their security systems (Sasso, 2014). The public outrage in the Target case also spiked, with numerous lawsuits and social media campaigns to boycott Target. Yet confusion and contestation over who "owned" this precursor event led to delayed response.

Media coverage typically spikes when hacks are made public (sometimes made by journalists themselves). Consumers of Equifax turned to social media (Lieber, 2017), the public called for boycott of Facebook after the

Cambridge Analytica scandal (Lang, 2018), public anger spilled over into the streets and even to social media in the US and Europe after Snowden's revelations, and lawsuits were filed in several cases including Target's data breach (Zetter, 2014). The media, including *The New York Times* (US) and *The Guardian* (UK), repeatedly covered the progress of cases and documented the frustration amongst consumers on the receiving end.

These reactions by the public and media were followed by broader expert attention—a type of "we told you so" reaction. After the 2014 Sony hack, security expert Brian Krebs urged the US to see this incident as "a wake-up call" (Krebs, 2014). Similarly, after Yahoo publicly announced their system breach in 2016, Krebs argued that he had noted these problems previously and "saw this coming" (Krebs, 2016). Chris Hughes, co-founder of Facebook, walked away from his former company to urge society to fight against the "asymmetrical power of firms" and demanded more accountability in regard to data usage (Bursztynsky, 2019). A similar message comes from Chris Wylie, who exposed the Cambridge Analytica scandal. Wylie argues for stricter measures to be taken to prevent undetected or unnoticed data compromises (Wong, 2019).

A paradox exists when considering the crisis attention paid to Big Data. Consumers enjoy the daily conveniences associated with Big Data—tracking software, swift banking, purchasing suggestions. They tend to downplay the risks at an everyday level (Griffore, 2018). But when those risks actually manifest themselves, in the form of abuse and breaches, outrage quickly follows. At those moments, which we delve into below, the promise and pitfalls of today's reliance on Big Data becomes dramatically apparent. Anger and shock are directed toward companies and citizens demand governmental action to stop this "unprecedented threat to human freedom" (Zuboff, 2020). Media attention follows, and action is promised. Yet these "precursor events" are just the symptoms of a much deeper underlying crisis creeping through time and space.

5.6 Response

This is not to suggest a complete lack of action. In fact, there appears to be a pattern here. In the immediate aftermath of a precursor event, governments demand action by placing blame on private firms. Penalties are handed out and courts deliver verdicts (sometimes years after an incident). Task forces are formed at national and international levels to investigate the "problem". Indeed, our analysis of this creeping crisis reveals another pattern: after initial outrage and anger at firms, the blame game shifts toward governments. Tough questions are asked why politicians had not been doing more, from the start.

The Cambridge Analytica scandal led to government hearings and investigations across the world. In 2018, the US began congressional hearings (Wichter, 2018) with a key group for US senators led by Senator Richard Blumenthal, calling for punishment and the need to restore trust (Confessore, 2018). In the UK, British lawmakers investigated what role Cambridge Analytica and Facebook might have played in the Brexit referendum (Confessore, 2018), which was followed by Britain's Information Commissioner's Office (ICO) imposing a fine of 500,000 GBP for the Facebook data breach of millions of British users' personal data (Reuters, 2019). And in the EU, the European Parliament conducted hearings and a new momentum drove negotiations to complete the General Data Protection Regulation (Kozlowska, 2018). Facebook attempted to make amends by imposing new standards on data harvesting. But these promises were viewed with skepticism because of previous resistance to change and the fact that Facebook's main revenue stream comes from selling the private data they accrue (Zuboff, 2019). Lawmakers in the US state of California adopted sweeping new data privacy laws, to allow some degree of consumer control over data—even if this does not stop what companies are allowed to do with our private data.

When a scandal surrounding Big Data is deemed to have national security or criminal implications, law enforcement gets involved. Target corporation was taken to task by government authorities, for instance. After nearly four years of hearings (Sasso, 2014), official resignations (Bronner, 2014; Harris, 2014) and constant consumer lawsuits (Zetter, 2014), Target was fined 18.5 million USD in March 2017 (Hong, 2017) (despite the fact that the data was never retrieved). Following the Sony hack in 2014, the US FBI was one of the first to be informed of the breach and started an investigation (Laughland & Rushe, 2014). The same occurred after the Marriott data breach in 2018, where the FBI was informed about the breach before the public (Shepardson, 2019). Following Snowden's revelations in 2013, the US National Security Administration began investigating its own security systems in 2014 (Tucker, 2016) while a host of international conferences considered regulatory implications (Travis, 2015).

As different national actors respond to and investigate precursor events, we witness international organizations increasing their involvement as well. The EU worked together and implemented the General Data Protection Regulation (GDPR) in 2018 following the Cambridge Analytica scandal (Kozlowska, 2018). Similarly, international cybersecurity organizations worked to issue guidelines for users after the WannaCry ransomware attack, arguing that the threat had worldwide implications (Baraniuk, 2017). The UN and OECD publish regular warnings based on task forces and investigations.

To be sure, governments appear to act. But these are less regulatory (outside of California and the EU's GDPR rules) and more punitive. In a very limited number of cases, we witness intervention *despite* declining public attention (an anomaly according to the creeping crisis framework). Although international lawmakers attempt to design collective solutions, national lawmakers appear to have a longer engagement. In investigating the Equifax breach, the US Justice Department in 2020 found Chinese hackers to be responsible, three years after the breach (Warzel, 2020). In investigating the Sony hack, the US filed complaints against North-Korean hacker Park Jin Hyok in 2018, four years after the breach (Bing & Lynch, 2018). At the same time, he was also charged with involvement in the WannaCry ransomware attack.

Target agreed to pay 18.5 million USD in 2017 (Hong, 2017), Yahoo in 2019 had to agree to pay-out to US and Israeli citizens who were affected by their data breach (Martinez, 2019), Marriott in 2019 was fined over 100 million GBP over GDPR breach (Sweney, 2019) and Facebook had to pay multiple fines to Brazil, UK and the US. Thus, when public attention fades and government oversight dissolves, the courts are the only ones left to close these cases. Longer-term solutions are difficult to find, and governmental regulators remain behind the regulatory curve.

5.7 Conclusion

Big Data represents the quintessential creeping crisis: a long evolution of a potential threat propelled by intersecting conditions, a constant presence in society, periodic attention from experts and officials, and yet no sustained action.

Three poignant aspects of this case help to enrich our understanding of creeping crises. First, the rise of Big Data as a threat took place because of a virtuous cycle of interacting developments. These developments relate to the rise of technology in the global economy. The accumulation of Big Data and the opportunities to manipulate it for good or ill were initially considered as mere side-effects. Few noticed or cared about the early warnings of experts. Damage capacity seemed small; the risk was complex rather than clear. Big Data was thus allowed to arrive, unheralded, on the crisis scene. Unlike other cases in this book, the development was purely technological, rather than stemming from the human-ecology interface, such as climate-change related crisis.

Second, Big Data typifies the crisis-attention cycle seen in other chapters in this volume, including Covid-19 (see Chap. 7) and climate-induced migration (see Chap. 8). Precursor events start with a failure to act, despite warnings (which were only clear "warnings" in hindsight). Failure to act is followed by unauthorized access to large-scale databases, which, often after significant delays, are then publicly disclosed. This disclosure leads to a spike in media attention and public outrage, which, in turn, generates political attention. This outrage draws attention to privacy violations and major breaches in personal integrity (civil liberties). But as time passes, the sense of urgency fades and political attention shifts to other issues. Rather than large-scale, regulatory responses, the court system usually ends up holding the bag, imposing moderately sized fines. More recently, expert groups and media outlets have become more proactive, highlighting the major risks at stake (data privacy reporting is now a priority issue for *The New York Times*, for instance). The international community (UN, EU, etc.) focuses on the crisis for a more sustained period but, with the exception of the EU, has little authority to act.

Third, a concerted crisis response fails to materialize. Why the lack of sustained action? What might be the tipping point at which "enough is enough," or the number of precursor events becomes too hard to ignore? Several explanatory factors deserve further attention. One is dependence. Officials do not act upon this creeping crisis because essential societal functions are at stake. These functions—criminal analysis, energy distribution, and food supply networks, for instance—are data driven. The ostensible benefits of data-driven public policies (by governments) and marketable consumer profiles (by firms) are sold in rosy terms and optimistic language. The technologies driven by, and driving, data accumulation are used daily by individual citizens: from mapping apps to information searches. To abolish these technologies is difficult, and even to regulate them comes with serious trade-offs.

Another reason for a lack of interest, related to dependence, is vested interests. The companies that have shifted their business model toward the mining of Big Data for commercial and security use as the primary purpose (Facebook, Alphabet, TikTok, etc.) carry huge economic weight in their respective countries. Their representatives sway politicians' opinions away from acting to avoid a future crisis—the 2018 testimony of Mark Zuckerberg in the US Congress carried exactly that message.

More concretely, there is no shared definition of the problem (cf. Wildavsky, 1992). Not only do vested interests and societal dependencies lead to a continuous reframing of the risks of Big Data, but the multifaceted nature of the problem also makes a simple threat assessment difficult. Is this an economic problem, a security problem, a moral problem, or a personal problem? The various precursor events elicit a wide range of perspectives and opinions, despite the fact that the problem overall is growing. Perhaps only a "big one"—the eventual societal-wide crisis toward which we are creeping—will be enough to focus attention and command a sufficient response.

References

Abbate, J. (1999). The electrical century. *Proceedings of the IEEE, 87*(9), 1695–1698.

Andrew, O. (2018). The history and evaluation of the smartphone: 1992–2018. Retrieved November 30, 2019, from https://www.textrequest.com/blog/history-evolution-smartphone/

Baraniuk, C. (2017, May 15). Should you pay the WannaCry ransom?. *BBC News*. Retrieved November 20, 2020, from https://www.bbc.com/news/technology-39920269

Bing, C., & Lynch, S. N. (2018, September 6). U.S. charges North Korean hacker in Sony, WannaCry cyberattacks. *Reuters*. Retrieved November 20, 2020, from https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W

Boin, A., & Lodge, M. (2019). The new Twilight Zone between crisis and risk management. *Risk and Regulation*, Spring, LSE CARR Newsletter. Retrieved September 15, 2020, from www.transcrisis.eu.

Bride, E. (2011). The IBM personal computer: A software-driven market. *IEEE Computer Society, 44*(8), 34–39.

Bronner, D. W. (2014, May 5). Target CEO steps down after 35 years. *The Atlantic*. Retrieved November 20, 2020, from https://www.theatlantic.com/business/archive/2014/05/target-ceo-steps-down-over-massive-data-breach/361696/

Buck, R. (2011, April 27). Standing at the edge of the precipice of consumer trust. *ClickZ Newsletter*, p. 2.

Bursztynsky, J. (2019, June 17). Facebook co-founder Chris Hughes: I still consider Mark Zuckerberg a friend, but his 'power has grown too big'. *CNBC*. Retrieved November 20, 2020, from https://www.cnbc.com/2019/06/17/facebook-co-founder-chris-hughes-zuckerberg-a-friend-but-too-powerful.html

Ceruzzi, P. E. (2010). 'Ready or not, computers are coming to the people': Inventing the PC. *OAH Magazine of History, 24*(3), 25–28.

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. *The New York Times*. Retrieved November 20, 2020, from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

DePillis, L., & Sherman, I. (2018, October 4). Amazon's extraordinary 25-year evaluation. *CNN Business*. Retrieved November 20, 2020, from https://edition.cnn.com/interactive/2018/10/business/amazon-history-timeline/index.html

Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times Magazine*. Retrieved November 20, 2020, from https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. *Journal of Business Research, 69*, 897–904.

Grable, J. E., & Lyons, A. C. (2018). An introduction to Big Data. *Journal of Financial Service Professionals, 72*(5), 17–20.

Griffore, R. J. (2018). The significance of Big Data literacy in higher education. *Journal of Behavioral and Social Sciences, 5*, 231–236.

Gruetzemacher, R. (2018). Rethinking AI strategy and policy as entangled super wicked problems. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society (AIES '18)* (p. 122). New York, NY: Association for Computing Machinery.

Hackenberger, B. K. (2019). Data by data, Big Data. *Croatian Medical Journal, 60*, 290–292.

Hacking, I. (2015). Biopower and the avalanche of printed numbers. In V. W. Cisney & N. Morar (Eds.), *Biopower: Foucault and beyond* (pp. 65–80). Chicago: University of Chicago Press.

Harris, E. A. (2014, April 29). After data breach, Target plans to issue more secure chip-and-PIN cards. *The New York Times*. Retrieved November 20, 2020, from https://www.nytimes.com/2014/04/30/business/after-data-breach-target-replaces-its-head-of-technology.html

Hong, N. (2017, May 23). Target to pay $18.5 Million to settle massive 2013 data breach. *The Wall Street Journal*. Retrieved November 20, 2020, from https://www.wsj.com/articles/target-to-pay-18-5-million-to-settle-massive-2013-data-breach-1495561952

Kozlowska, I. (2018). *Facebook and data privacy in the age of Cambridge Analytica*. Retrieved November 20, 2019, from https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/

Krebs, B. (2014). *FBI: North Korea to blame for Sony hack*. Retrieved March 4, 2020, from https://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/

Krebs, B. (2016). *Yahoo: One billion more accounts hacked*. Retrieved March 3, 2020, from https://krebsonsecurity.com/2016/12/yahoo-one-billion-more-accounts-hacked/

Lang, C. (2018, March 22). 'It's not good.' Mark Zuckerberg discusses the #DeleteFacebook Campaign. *Time*. Retrieved November 20, 2020, from https://time.com/5210799/mark-zuckerberg-addresses-delete-facebook-campaign-after-cambridge-analytica/

Laughland, O., & Rushe, D. (2014, December 19). Sony cyber attack linked to North Korean government hackers, FBI says. *The Guardian*. Retrieved November 20, 2020, from https://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official

Lieber, R. (2017, September 12). Equifax, bowing to public pressure, drops credit-freeze fees. *The New York Times*. Retrieved November 20, 2020, from https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html

Martinez, G. (2019, October 15). Yahoo could owe you up to $358 for data breaches. Here's how to file your claim. *Time*. Retrieved November 20, 2020, from https://time.com/5700738/yahoo-settlement-how-to-file-claim/

Microsoft. (2017). Microsoft Security Bulletin MS17-010-Critical. Retrieved November 20, 2020, from https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010

Mims, F. M. (1985). The tenth anniversary of the Altair 8800. *Computer and Electronics*.

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS*. Report by the Comptroller and Auditor General for the Department of Health. London: National Audit Office.

Newman, L. H. (2017, September 14). Equifax officially has no excuse. *Wired*. Retrieved November 20, 2020, from https://www.wired.com/story/equifax-breach-no-excuse/

O'Neill, C. (2016). *Weapons of math destruction: How Big Data increases inequality and threatens democracy*. New York: Penguin.

O'Reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & Strategies*, no. 65, 1st quarter, pp. 17–37.

Ortiz-Ospina, E. (2019). The rise of social media. Retrieved September 18, 2019, from https://ourworldindata.org/rise-of-social-media

Perrow, C. (1984). *Normal accidents*. New York: Basic Books.

Reuters. (2019, October 30). Facebook agrees to pay UK fine over Cambridge Analytica scandal. *Reuters*. Retrieved November 20, 2020, from https://www.reuters.com/article/us-facebook-privacy-britain/facebook-agrees-to-pay-uk-fine-over-cambridge-analytica-scandal-idUSKBN1X913O

Sasso, B. (2014, March 25). Senate report: Target could have prevented massive hack. *The Atlantic*. Retrieved November 20, 2020, from https://www.theatlantic.com/politics/archive/2014/03/senate-report-target-could-have-prevented-massive-hack/457125/

Shepardson, D. (2019, March 4). Marriott CEO to testify before U.S. Senate panel on data breach. *Reuters*. Retrieved November 20, 2020, from https://www.reuters.com/article/us-senate-marriott-intnl/marriott-ceo-to-testify-before-u-s-senate-panel-on-data-breach-idUSKCN1QL25U

Sweney, M. (2019, July 9). Marriott to be fined nearly £100m over GDPR breach. *The Guardian*. Retrieved November 20, 2020, from https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico

Szoldra, P. (2016, June 10). A hacker explains why you shouldn't believe North Korea was behind the massive Sony hack. *Business Insider*. Retrieved November 20, 2020, from https://www.businessinsider.com/north-korea-sony-hack-2016-6?r=US&IR=T

Travis, A. (2015, June 15). Snowden leak: Governments' hostile reaction fueled public's distrust of spies. *The Guardian*. Retrieved November 20, 2020, from https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies

Tucker, P. (2016, September 18). Can the NSA stop the next Snowden? *The Atlantic*. Retrieved November 20, 2020, from https://www.theatlantic.com/international/archive/2016/09/nsa-snowden/500345/

Warzel, C. (2020, February 10). Chinese hacking is alarming. So are data brokers. *The New York Times*. Retrieved November 20, 2020, from https://www.nytimes.com/2020/02/10/opinion/equifax-breach-china-hacking.html

Wichter, Z. (2018, April 12). 2 days, 10 hours, 600 questions: What happened when Mark Zuckerberg went to Washington. *The New York Times*. Retrieved November 20, 2020, from https://www.nytimes.com/2018/04/12/technology/mark-zuckerberg-testimony.html

Wildavsky, A. (1992). *Speaking truth to power*. New Brunswick: Transaction Publishers.

Wolcott, M. (2008, May 1). What is Web 2.0? *CBS NEWS*. Retrieved November 20, 2020, from https://www.cbsnews.com/news/what-is-web-20/

Wong, J. C. (2019, March 18). The Cambridge Analytica scandal changed the world—But it didn't change Facebook. *The Guardian*. Retrieved November 20, 2020, from https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

Zetter, K. (2014, January 17). Target got hacked hard in 2005. Here's why they let it happen again. *Wired*. Retrieved November 20, 2020, from https://www.wired.com/2014/01/target-hack/

Zuboff, S. (2019). *The age of surveillance capitalism*. New York: Profile Books.

Zuboff, S. (2020, January 24). You are now remotely controlled. *The New York Times*. Retrieved November 20, 2020, from https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html