Digital Citizenship: Misinformation & Data Commodification in the Twenty-First Century

Digital Citizenship: Misinformation & Data Commodification in the Twenty-First Century

Misinformation & Data Commodification in the Twenty-First Century

SARAH GIBBS AND ADRIAN CASTILLO

Contents

Digital Citizenship: Misinformation & Data Commodification in the Twenty-First Century

SARAH GIBBS AND ADRIAN CASTILLO

MHC Libraries Digital Citizenship Series:
Volume 1
by
Sarah Gibbs, PhD, MLIS & Adrian Castillo, MLIS

Introduction

SARAH GIBBS

"The connection between surveillance capitalism and disinformation lies in the increased capacity of platforms to microtarget messages and alter behavior without people being aware of their influence."

—Paul Starr; "The Flooded Zone: How We Became More Vulnerable to Disinformation in the Digital Era" (2020)

In the twenty-first century, online information seekers are increasingly obliged to arm themselves against countries, companies, and rogue bad actors that disseminate disinformation and indiscriminately harvest personal data. The still largely unregulated flow of content on the Internet means these parties can covertly influence user behaviour, and thereby endanger everything from election integrity to public health. *Digital Citizenship, Vol.1: Misinformation & Data Commodification in the Twenty-First Century* is Medicine Hat College (MHC) Library's contribution to growing efforts to address the gap in post-secondary education concerning the socio-political and economic dimensions of online life.

The goals for the text, and the associated instructional program for MHC students, are:

1. To provide readers and/or session participants with the foundational knowledge required to understand the mechanisms that enable online communication and that monetize its content
2. To give readers and/or session participants strategies to navigate effectively what is often a confusing and divisive information environment, and to become positive actors within it

3. To help widen the purview of Information Literacy (IL) instruction to encompass the socio-political dimension of information
4. To contribute both to the discussion around Public Interest Technology (PIT) in post-secondary education and to the development of quality Open Educational Resources (OER) in Library and Information Studies

The book includes two sections. Part I considers the prevalence of misinformation, disinformation, and fake news in the twenty-first-century media environment, and offers readers means to become more savvy information consumers, including tips for recognizing both fake news websites and the rhetorical strategies on which hyper-partisan reporting relies. Part II examines the rise of what Shoshana Zuboff has termed "surveillance capitalism": the creation of markets for the personal data search engine and social media companies capture when users engage with their platforms. The section guides readers through assessing the terms and conditions associated with different apps and describes the approaches individuals and governments can adopt in order to reclaim ownership of online data.

Among MHC's strategic goals is the desire to equip students with transferrable skills that will serve them well in the job market. The Library Services team believes that, in a knowledge economy, there is no more valuable work, or life, skill than robust information literacy.

PART I

PART I: MISINFORMATION

"[A]s the vilest writer hath his readers, so the greatest liar hath his believers: and it often happens, that if a lie be believed only for an hour, it hath done its work, and there is no further occasion for it. Falsehood flies, and truth comes limping after"

–Jonathan Swift; "The Art of Political Lying" (1710)

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=5#h5p-32

"[A]ny attack on [...] the concept of objective truth [...] threatens in the long run every department of thought."

George Orwell
"The Prevention of Literature" (1946)

In the "post-truth" twenty-first century, our information environment is fraught. Controversies concerning "fake news" and the authority of experts shape our daily lives; fringe media attack the validity of democratic processes and COVD-19 misinformation contributes to preventable deaths and imperils public health. In the digital sphere, all sources—whether reputable or not—can appear equal. According to W. Lance Bennett and Steven Livingston in their work, *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States* (2020):

> Democracies around the world face rising levels of disinformation. The intentional spread of falsehoods and related attacks on the rights of minorities, press freedoms, and the rule of law all challenge the basic norms and values on which institutional legitimacy and political stability depend. (p. xv)

The authority and reliability of information is no longer a strictly academic concern; the sources of disinformation are numerous and can include communications from politicians and political parties, and messaging from groups spreading conspiracy theories,

attacking the "scientific evidence surrounding important issues such as climate change [...] [and] [inventing] stories to inflame existing social and political conflicts" (Bennett and Livingston, 2020, p. xv). This chapter aims to equip readers with the skills they need to assess information in the world at large, whether the source is a post on social media, a report on the nightly news, or a political candidate's speech.

After reviewing the chapter, readers will be able to:

- Define "misinformation," "disinformation," and "fake news"
- Discuss historical instances of disinformation
- Describe the conditions that have contributed to the current boom in mis- and disinformation
- Identify and respond effectively to disinformation and fake news, both as information consumers and engaged twenty-first-century citizens

Some portions of the text contain a section entitled "The Deep Dive." The materials are optional readings and/or video content for those who wish to investigate a topic further.

Activity

Consider the headlines below. Which seem to be true? Don't look it up. Just go with your gut.

"Subway bread is not bread, Irish court rules" (*The Guardian*; 2020)

"Pope Francis shocks world, endorses Donald Trump for president" (*Ending the Fed*; 2016)

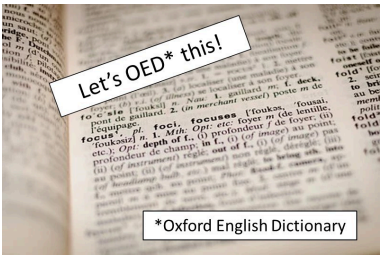
"Private Florida School Says it Will Not Employ Anyone who has Received Covid-19 Vaccine" (*The Globe and Mail*; 2021)

"FBI agent suspected in Hillary email leaks found dead in apartment murder-suicide" (*Denver Guardian*; 2016)

Remember your answers. We'll come back to them.

2: Definitions

SARAH GIBBS



Unsure of the difference between misinformation and propaganda? Wondering when "fake news" became a "real thing"? Check out the handy definitions below, courtesy of the Oxford English Dictionary and scholars in information studies.

Misinformation

Wrong or misleading information. Nicole A. Cooke (2018) notes that misinformation may be incorrect, or simply incomplete, uncertain, or ambiguous. Misinformation may retain some value, depending on the context (Cooke, 2018). Its creators may be unaware that the information is false.

Disinformation

Deliberately false information, especially that incorrect information supplied by a government or its agent to a foreign power or to the media, with the intention of influencing the policies or opinions of those who receive it. Cooke (2018) suggests that "disinformation is carefully planned, can come from individuals or

groups, can be circulated by entities other than the creators [...] [(e.g. news organizations)], and is typically written or verbal information" (p.6). She argues that "the key to disinformation is that it is created with malicious or ill intent" (pp. 6-7).

Fake News

Originally U.S. news that conveys or incorporates false, fabricated, or deliberately misleading information, or that is characterized as or accused of doing so. The term was widely popularized during and after the 2016 U.S. presidential election campaign, and since then has been used in two main ways: to refer to inaccurate stories circulated on social media and the Internet, especially ones that serve a particular political or ideological purpose; or to seek to discredit media reports regarded as partisan or untrustworthy.

Fun Fact: The first recorded use of the term "fake news" dates from 7 February 1890, when a piece in the Milwaukee Daily Journal *declared, "That mine story is one of the greatest pieces of fake news that has been sprung on the country for a long time."*

Propaganda

Information of a prejudiced or disingenuous [insincere] nature that is used to encourage a political cause or point of view (Cooke, 2018, p. 4). Propaganda is information that is subjective and is used primarily to influence the target audience and further an agenda, often by presenting facts selectively (perhaps lying by omission), or by using coded or suggestive messages or language to elicit [generate] an emotional response, as opposed to a rational response. (p.4)

Fun (?) Fact: "The term 'propaganda' originated in the early seventeenth century, when Pope Gregory XV established the Sacra Congregatio de Propaganda Fide—the Sacred Congregation for the Propagation of the Faith. The Congregation was charged with spreading Roman Catholicism through missionary work across the world." (O'Connor & Weatherall, 2019, p. 97)

Pseudoscience

A branch of knowledge or a system of beliefs mistakenly regarded as based on scientific method or having the status of scientific truth, or study or research that is claimed as scientific but is not generally accepted as such.

Fun Fact: The first recorded use of the term "pseudoscience" was in 1796; the term was applied to alchemy, a "science" that claimed to be able to turn lead into gold.

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=39#h5p-4

3. History

SARAH GIBBS

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=46#h5p-31

Ever heard the phrase "nothing is certain but death and taxes"? It's a paraphrase of a statement attributed to Benjamin Franklin, the American inventor and politician. Ben could have added "disinformation" to his list, as it's been around since the beginning of time. Check out some further historical examples of disinformation below, as described by Cailin O'Connor and James Owen Weatherall in their book, *The Misinformation Age: How False Beliefs Spread* (2019).

It featured in the American War of Independence:

"In the decades immediately before and after the American Revolution [...], partisans on all sides attacked their opponents through vicious pamphlets that were often filled with highly questionable accusations and downright lies" (p.152).

It made people think they could get a holiday home on the moon:

"In 1835, the *New York Sun*, a politically conservative but generally reputable newspaper, published a series of six articles asserting that the English astronomer John Herschel had discovered life on the moon. The articles claimed to have been reprinted from an Edinburgh newspaper and contained a number of alleged quotes

from Herschel. They even included illustrations of winged hominids Herschel was said to have seen. Needless to say, there is no life on the moon—and Herschel never claimed to have found it. The articles were never retracted. (Compare these claims to ones made by a guest on Alex Jones's Infowars radio show in June 2017 to the effect that NASA is running a child slavery colony on Mars)" (p.153)

Edgar Allan Poe Did it!

In 1844, "Edgar Allan Poe published a story in the *Sun* in which he described (as factual) a trans-Atlantic hot-air balloon journey by a famous balloonist named Monck Mason. This [...] never occurred. (The article was retracted two days later.)" (p.153)

Supplemental Video: Fake News and Biography: Edgar Allan Poe—Buried Alive (https://www.pbslearningmedia.org/resource/poe17-ela-fakenews/fake-news-and-biography-edgar-allan-poe-buried-alive/). PBS.

It started a war:

"[Disinformation and] [f]ake news arguably launched the Spanish American War. After the USS *Maine*—a US warship sent to Havana in 1898 to protect American interests while Cuba revolted against Spain—mysteriously exploded in Havana Harbor, several US newspapers [...] began to run sensational articles blaming Spain for the explosion and demanding a war of revenge. (The actual cause of the explosion was and remains controversial, but concrete evidence has never been produced that Spain was involved.) Ultimately, spurred in part by pressure from the news media, the US government gave Spain an ultimatum that it surrender Cuba or face war—to which it responded by declaring war on the United States." (pp. 152-153)

It caused preventable deaths:

"A classic example of [disinformation] is the campaign by tobacco

companies during the second half of the twentieth century to disrupt and undermine research demonstrating the link between smoking and lung cancer. [...] Tobacco firms paid 'experts' to create the impression that there was far more uncertainty and far less consensus than there actually was. This campaign successfully delayed, for a generation or more, regulation and public health initiatives to reduce smoking." (p.10)

If disinformation has always been around, why does the situation seem so much worse today? Read on to find out.

Supplementary Information

Want to learn more about the Vegetable Lamb? Check out the links below!

https://www.nybg.org/poetic-botany/barometz/

https://www.youtube.com/watch?v=Ff-5B47ykC0

4.1 Misinformation Today: The Internet

SARAH GIBBS

Broadcast Capability

> "[F]ake news [and disinformation] ha[ve] been with us for a long time. And yet something has changed—gradually over the past decade, and then suddenly during the lead-up to the 2016 UK Brexit vote and US election." —Cailin O'Connor & James Owen Weatherall; *The Misinformation Age* (2019)

What changed? Well, where once people who wanted to mislead the public had to shout to be heard over a mass of other voices, social media has now given online bad actors a megaphone. Communication is instant, international, and unlimited.

Consider the difference from when New York City newspapers were advocating for war with Spain at the end of the nineteenth century:

> In 1898, when the *New York World* and *New York Journal* began agitating for war, they had large circulations. [...] But their audience consisted almost exclusively of New Yorkers—and not even all New Yorkers, as the better-respected *Times*, *Herald Tribune*, and *Sun* also had wide readerships. Regional newspapers outside New York generally did not pick up the *World* and *Journal* articles calling for war with

> Spain. Although the stories surely influenced public opinion and likely contributed to the march toward war, their impact was limited by Gilded Age media technology. (O'Connor & Weatherall, 2019, p. 154)

No such limitations exist today, and there are few—if any—checks on the authority or credentials of people sharing information on social media. If I want to convince the world that the members of the Canadian Supreme Court have been replaced by cheese-eating space aliens from Neptune, all I have to do is start a Twitter account. My warnings about Gouda-scented extraterrestrial domination can circle the globe in seconds.

Economics

> "The first fifty years of Silicon Valley, the industry made products: hardware, software sold to customers.

> Nice simple business. For the last ten years, the biggest companies of Silicon Valley have been in the business of selling their users." Roger McNamee. Facebook (early investor); *The Social Dilemma*, 12:50.

Social media companies make money off our attention. How? When we engage with content online, we also engage with advertising. Marketing companies pay Facebook, Twitter, and Instagram to feature their ads. Aza Raskin, a former employee of Firefox and Mozilla Labs and the inventor of the "infinite scroll" states, "Because we don't pay for the products we use, [because] advertisers pay for the products we use, advertisers are the customers. We're the thing being sold." (*The Social Dilemma*, 13:07).

For social media enterprises, the most important thing is that users see and respond to ads. Melodramatic, strange, or politically inflammatory content often gets the most attention, and therefore generates the most ad revenue. Essentially, the more extreme the news story, the better. YouTube has stated that videos made available via its recommendation algorithm account for over 70% of viewing time on the platform (Starr, 2020). Sensational videos get more "clicks," and are therefore recommended more heavily and receive even more views; the cycle is self-reinforcing and extremist material circulates heavily. W. Lance Bennett and Steven Livingston note that "social media's propensity to algorithmically push extremist content and to draw likeminded persons together with accounts unburdened by facts" (2020, vviii) has contributed significantly to increased consumption of disinformation and fake news.

According to Paul Starr (2020), until recently, social media companies "had no incentive to invest resources to identify disinformation, much less to block it" (p. 80). Profits outweighed

ethics; disinformation paid well. Changes are in the works, however. As of May 2021, Facebook and Twitter enacted policies to limit the reach of influential users (i.e. high profile persons and/or those with large numbers of followers) who repeatedly circulate mis- or disinformation (Ovide, 2021a). Such users' posts will feature less heavily in news feeds and accounts may be suspended for ongoing violations.

"Virality favors false and emotional messages."

Paul Starr; "The Flooded Zone: How We Became More Vulnerable to Disinformation in the Digital Age" (2020)

Supplemental Video: *YouTube Algorithms: How to Avoid the Rabbit Hole* (https://www.pbslearningmedia.org/resource/youtube-algorithms-above-the-noise/youtube-algorithms-above-the-noise/). PBS.

Fringe Belief Reinforcement / Validation

So, I love *Pacific Rim* (2013), director Guillermo del Toro's mash-up of *Godzilla* and *Transformers*. Is it a good movie? No. Not at all. Talking to regular people in the real world has assured me that it's pretty terrible. If I happened, however, to find a website, Twitter feed, or Facebook group in which everyone (all ten members) believed that the film is a masterpiece, I might begin to think that all the *Pacific Rim* haters are deluded or perhaps even conspiring against me…

While online communities offer users considerable benefits, one of their downsides is that people with "fringe" beliefs can create spaces where their arguments go unchallenged by facts or evidence. Online communities are self-organizing and self-selecting, so the diversity of views and perspectives that characterize society "in real life" are rarely represented, and potentially anti-social or dangerous beliefs can take deeper root. Feeling that *Pacific Rim* is underappreciated is fairly harmless* (*film critics may disagree), but what about online communities whose beliefs center on hatred of particular political parties, countries or minorities, or who advocate violence? Online "fringe" groups are major sources of misinformation, disinformation, and fake news.

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here:

https://openeducationalberta.ca/digitalcitizenship/?p=49#h5p-2

4.2 Misinformation Today: The Media

SARAH GIBBS

Media Fracturing & Iterative Journalism

These days, we can choose our news.

In the past, sources of information were limited. If we wanted to find out about a new policy the government was enacting, we could read about it in the newspaper, listen to a report on the radio, or watch the news on TV. There were comparatively few newspapers, radio stations, or TV programs to choose from, and they all reported fairly similar information. Now, the options can appear limitless and news sources often disagree on basic questions of fact.

Our contemporary media environment is characterized by three important features:

1. **Personal Preference & Source Heterogeneity**—Something is "heterogeneous" when it is composed of diverse and / or dissimilar parts. The vast array of media outlets available today

means that our media environment is highly heterogeneous. Librarian Nicole A. Cooke (2018) describes the result of a broad array of choices in news outlets:

> With a simple click of the mouse, change of the channel, or file download, consumers can choose a news media outlet that is most aligned with their ideological preferences. This is fragmentation in news. It provides more choice and possible exposure to wider perspectives in the news, though at the cost of a radical increase in the amount of biased or unbalanced reports propagating in the mass media." (p. 13)

The need for online news sources to drive traffic to their sites in order to generate ad revenue, and their ability to act as "micro media" (p. 13) targeting a highly specific group of consumers, means that these sources tend to simply "give people what they want," framing and manipulating news stories in ways that appeal to their users. Many people remain entirely within their "media bubbles" and never seek out information from sources with different perspectives or political orientations. Being informed means gathering information from a variety of reputable sources.

2. **Disintermediation**—Essentially, the removal of intermediaries. Internet platforms greatly reduce or completely eliminate barriers for publishing "citizen-produced content" (Cooke, 2018, p. 13). New online media pathways bypass traditional "information gatekeepers," like professional journalists and fact-checkers. Cooke (2018) notes, "Disintermediation is yet another reason why fake news thrives, because information can travel from content producer to consumer in a matter of seconds without being vetted by intermediaries such as reputable news organizations" (p. 13-14).

3. **Iterative Journalism**—Iterative journalism is the practice whereby "media personalities [...] report[...] what they've heard, not what they have discovered or sought out directly" (Cooke, 2018, p. 12). Basically, it's when news outlets report information second-hand. The contemporary twenty-four-hour news cycle means that media sites are under incredible pressure to provide a continual stream of new information; as a result, they are often re-reporting stories they've found elsewhere on the web. The situation is a recipe for propagation of misinformation, disinformation, and fake news. Fallacious stories can enter the media "food chain" on local news blogs or sites that carry out little-to-no fact checking, and then work their way up to major media outlets.

> "When we open our ideas up to group scrutiny, this affords us the best chance of finding the right answer. And when we are looking for the truth, critical thinking, skepticism, and subjecting our ideas to the scrutiny of others works better than anything else. Yet these days we have the luxury of choosing our own selective interactions. Whatever our political persuasion, we can live in a 'news silo' if we care to. [...] These days more than ever, we can surround ourselves with people who agree with us. And once we have done this, isn't there going to be further pressure to trim our opinions to fit the group?"
>
> Lee Mcintyre; *Post-Truth* (2018)

Novelty Bias

On 22 June 2021, the *New York Times* newsletter, *On Tech with Shira Ovide* published some surprising statistics. According to Ovide:

- Americans spend about two-thirds of their TV time watching conventional television and just 6 percent streaming Netflix.
- Online shopping accounts for less than 14 percent of all the stuff that Americans buy.
- Only one in six U.S. employees works remotely.
- About 6 percent of Americans order from the most popular restaurant delivery company in the United States.

One of the reasons that the statistics may be surprising—we're generally under the impression that everyone streams Netflix and that we all buy everything from Amazon—is, according to Ovide, that " people (and journalists) tend to pay more attention to what's new and novel" (2021b, n.p.).

This tendency to report not what is representative of an entire situation or population, but rather what is atypical or interesting, is called "novelty bias," and it is particularly problematic in the area of science reporting.

Scientific research is a gradual process in which a series of methodologically sound and ethically rigourous studies build toward a generally accepted conclusion. On the way to this state of relative scientific certainty, unusual results and outlier studies will inevitably emerge. Quality science reporting will contextualize single atypical result sets within the context of the research in the area, and make clear that, while the study may be sound, the bulk of the research supports a different conclusion. Unfortunately, media items describing "scientific breakthroughs" do not always provide a balanced view of the discipline. Outlets focused on generating "clicks" and ad revenue may engage instead in selective evidence

dissemination and sensationalize the results (O'Connor & Weatherall, 2019, pp. 156). The story is not false, but its information is decontextualized and misleading. Propagandists rely heavily on selective evidence dissemination in order to shape public perception of issues.

> "There is a famous aphorism in journalism, often attributed to a nineteenth-century *New York Sun* editor, either John B. Bogart or Charles A. Dana: 'If a dog bites a man it is not news, but if a man bites a dog it is.' The industry takes these as words to live by: we rarely read about the planes that do not crash, the chemicals that do not harm us, the shareholder meetings that are uneventful, or the scientific studies that confirm widely held assumptions."
>
> Cailin O'Connor & James Owen Weatherall; *The Misinformation Age: How False Beliefs Spread* (2019)

Supplemental Video: Top Four Tips to Spot Bad Science Reporting (https://www.pbslearningmedia.org/resource/c7ab68b7-0f23-4888-952d-127ec9b71c17/top-4-tips-to-spot-bad-science-reporting-above-the-noise/). PBS

The Affective / Emotional Elements of Information

Have you ever been in this situation? Someone presents his or her side of an argument and supports it with evidence you can't refute, but nonetheless, you still feel that the other side or perspective is true. According to Nicole A. Cooke (2018):

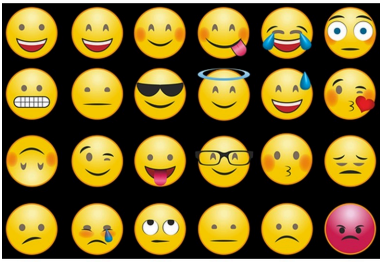
> One of the hallmarks of the post-truth era is the fact that consumers will deliberately pass over objective facts in favor of information that agrees with or confirms their existing beliefs, because they are emotionally invested in their current mental schemas or are emotionally attached to the people or organizations [that] the new information portrays. (p. 7)

Our desire for something to be true because we're emotionally invested in it often leads us to put aside rational thinking and commit to positions we know intellectually are false (Cooke, 2018). The television show *The Colbert Report* coined the term "truthiness" to describe the phenomenon: it's not true, but it feels like it is (Cooke, 2018).

Disinformation and fake news often rely on people responding

emotionally, rather than rationally, to news items. Taking a step back when you encounter news that makes you angry or afraid and ensuring that the story comes from a reputable source and cites reliable evidence can help you avoid falling prey to the emotional manipulation of online bad actors.

Feelings



The World's Worst Fact Checkers

Cognitive Bias

> "We are all beholden to our sources of information. But we are especially vulnerable when they tell us exactly what we want to hear."
>
> Lee Mcintyre; *Post-Truth* (2018)

An interactive H5P element has been excluded from this version of the text. You can view it online here:

https://openeducationalberta.ca/digitalcitizenship/?p=53#h5p-29

Above the Noise. (2017, *May 3*). Why do our brains love fake news? *[Video]. YouTube, https://youtu.be/dNmwvntMF5A.*

Check out Lee Mcintyre's (2018) description of two common manifestations of cognitive bias.

The Backfire Effect

"The 'backfire effect' is based on experimental work by Brendan Nyhan and Jason Reifler, in which they found that when partisans were presented with evidence that one of their politically expedient beliefs was wrong, they would reject the evidence and 'double down' on their mistaken belief. Worse, in some cases the presentation of refutatory evidence caused some subjects to *increase* the strength of their mistaken beliefs. [...] Some have described trying to change politically salient mistaken beliefs with factual evidence as 'trying to use water to fight a grease fire.' [...] / [However], even the strongest partisans will eventually reach a 'tipping point' and change their beliefs after they are continually exposed to corrective evidence." (pp. 48-51)

The Dunning-Kruger Effect

"The Dunning-Kruger effect (sometimes called the 'too stupid to know they're stupid' effect) is a cognitive bias that concerns how low-ability subjects are often unable to recognize their own ineptitude. Remember that, unless one is an expert in everything, we are probably *all* prone to this effect to one degree or another. [...] In their 1999 experiment, David Dunning and Justin Kruger found

that experimental subjects tended to vastly overestimate their abilities, even about subjects where they had little to no training. [...] In intelligence, humor, and even highly skilled competencies such as logic or chess, subjects tended to grossly overrate their abilities. Why is this? As the authors put it, 'incompetence robs [people] of their ability to realize it...The skills that engender competence in a particular domain are often the very same skills necessary to evaluate competence in that domain—one's own or anyone elses's.' The result is that many of us simply blunder on, making mistakes and failing to recognize them. [...]

[...] Perhaps this is the most shocking thing about the Dunning-Kruger result: the greatest inflation in one's assessment of one's own ability comes from the lowest performers." (pp. 51-53)

The Deep Dive

"The Psychology That Leads People to Vote for Extremists & Autocrats: The Theory of Cognitive Closure"

DANIELE ANASTASION

The New York Times, 30 November 2016

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=53#h5p-5

4.3 Misinformation Today: Social & Political Polarization

SARAH GIBBS

Social & Political Polarization

> "By 'nationalism' I mean first of all the habit of assuming that human beings can be classified like insects and that whole blocks of millions or tens of millions of people can be confidently labelled 'good' or 'bad.' But secondly—and this is much more important—I mean the habit of identifying oneself with a single nation or other unit, placing it beyond good and evil and recognizing no other duty than that of advancing its interests."
>
> —George Orwell; "Notes on Nationalism" (1945)

That the political situation in Europe in 1945—when Fascist states were being dismantled and the Iron Curtain was descending across the eastern frontier—could bear any similarity to our present socio-political reality may at first be difficult to believe. Nonetheless, the habit of mind that George Orwell describes in his 1945 essay "Notes on Nationalism" has reappeared in the twenty-first century. We live in an age of political polarization, that is, a period in which many people's views have moved to the extreme right or left of the political spectrum. Adherents view their own side as unquestionably correct and virtuous, and consider believers in the contrary position to be fundamentally different from themselves. They refuse to

consider dialogue or compromise with the other side, and may even advocate violence against opponents. Contemporary political discourse is often fundamentally binaric; issues, parties and people are either absolutely good or absolutely bad, and anything done in the service of one's cause is acceptable.

The mentality Orwell describes effectively destroys civil discourse and leads to political deadlock; parties are unwilling to collaborate in the manner that the legislative process requires. Politically motivated violence becomes more likely because opponents have been thoroughly dehumanized. The condition of political polarization exists in a mutually reinforcing relationship with social media. Extremist, hyper-partisan content attracts more views, which radicalizes its consumers and causes them to seek out and produce similar content.

Supplemental Video: Facebook and the 2016 Election (https://www.pbslearningmedia.org/resource/fln36fd-soc-2016election/facebook-and-the-2016-election-the-facebook-dilemma/). PBS

The Deep Dive:

"Dear Facebook, This is How You're Breaking Democracy: A Former Facebook Insider Explains How the Platform's Algorithms Polarize Our Society" (5 October 2020)

TED Talk by Yaël Eisenstat, a former CIA Analyst and Facebook staffer

5.1 What to Do: Be Information Literate

SARAH GIBBS

Remember these headlines? Complete the activity to find out which news is fake!

> *An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=72#h5p-1*

If you didn't correctly identify the facts and fiction, you're not alone. Numerous studies indicate that our ability to identify fake news on the basis of "gut instinct" is very poor. We tend to need additional techniques and tools in order to root out disinformation.

> *An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=72#h5p-30*

Common Sense Media Ratings & Reviews. (2017, *January* 31). 5 ways to spot fake news *[Video]. YouTube, https://youtu.be/g2AdkNH-kWA*

While we encounter too much information on a daily basis to

critically assess every piece, for important issues, remember to subject stories and sources to scrutiny on a few points:

- Accuracy (Does the story clearly identify the sources of its information? Is it free of typographical errors like spelling and grammatical mistakes?)
- Authority (Is the source of the story a well-recognized news outlet or periodical? Are its credentials and funding sources openly identified and verifiable?)
- Purpose (Is the story click bait? Does the headline reflect its actual content?)

The number of fact-checking organizations in existence has grown significantly in the past few years. According to the Duke Reporters' Lab, between 2019 and 2020, the number of active fact-checkers grew 50%; 300 organizations around the globe now regularly verify the accuracy of the news (Stencel and Luther, 2020). Some of the best-known services that fact check the media are Snopes (https://www.snopes.com/), the *Washington Post* Fact Checker (https://www.washingtonpost.com/news/fact-checker/), Full Fact (https://fullfact.org/), and Fact Check (https://www.abc.net.au/news/factcheck/). You can visit the organizations' websites to see whether they've assessed stories you've encountered.

When in doubt, cross reference! If you're uncertain of the accuracy of information available in a particular news story, try to find the information in other sources, especially those that you know are reputable and that adhere to high standards of journalism.

Handy Cheat Sheet

Handout: Legito-Meter (https://static.pbslearningmedia.org/

media/media_files/33c5f7f1-59b8-4c93-a5a3-8219764ee9fc/61a395c0-a59a-4a7c-a333-d66bb5d10e54.pdf). PBS

The Deep Dive

Video: How to Fact-Check History (https://www.pbslearningmedia.org/resource/how-to-fact-check-history-video/retro-report/). PBS

Video: Deepfakes: Can You Spot a Phony Video? (https://www.pbslearningmedia.org/resource/above-the-noise-deep-fakes/above-the-noise-deep-fakes/). PBS

5.2 What to Do: Recognize the Rhetoric

SARAH GIBBS

False Equivalence

> *An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=75#h5p-28*

Above the Noise. (2017, *May* 3). Why do our brains love fake news? *[Video]. YouTube*, *https://youtu.be/dNmwvntMF5A*.

False Antithesis

Antithesis, according to our friend the OED, is "an opposition or contrast of ideas, expressed by using as the corresponding members of two [...] sentences or clauses, words which are the opposites of, or strongly contrasted with, each other." False antithesis occurs when someone presents two ideas that are not in fact in opposition and indicates that to choose or prefer one means you automatically deselect or dislike the other.

For example, someone could create a false antithesis between apples and bananas: "Apples vs. Bananas! Choose Your Side in the Battle Royale! Liking One Means Hating the Other!" You may prefer apples to bananas, but actually like both. The terms are not in opposition, so there's no need to choose one or the other.

While the fictitious fruit bowl throwdown won't undermine our societies any time soon, false antithesis applied to politics can do a lot of damage. Say, for example, someone creates a false antithesis like "Democracy or Socialism." Citizens of democratic societies are unlikely to state that they oppose democracy. Like "justice" or "accountability," democracy is generally acknowledged to be a good thing. If this antithesis were true, supporting democracy would mean fully renouncing socialism. Socialism, however, is simply a socio-economic model that emphasizes resource redistribution through taxation and the delivery of key services via government agencies. Whether or not a country is socialist has no connection to whether it is democratic. Sweden, a socialist country, is also a democracy. The propagator of the false antithesis wishes to present democracy as inseparable from free market capitalism.

Reframing

If facts were Barbie dolls, "framing" would be akin to picking out Barbie's clothes. If you dress Barbie as a firefighter, people may associate her with heroism and support the GoFundMe page she recently set up to pay for her trip to Fiji. They may open their wallets on the assumption that Barbie plans to do good and meaningful work in the South Seas. If you dressed her up as Cat Burglar Barbie, people might not be so quick to donate ("She's probably trying

to evade arrest!"). Barbie herself—that is, the facts of an incident, policy, or communication—remains unchanged. The manner in which she's dressed up and presented determines how people react.

Research has repeatedly demonstrated that the frame in which news is delivered—the context provided, the other news items to which it is linked, even the metaphors used to describe its content—greatly influence people's response to the facts and the political positions and activities they consequently advocate (Rathje, 2017; Thibodeau and Boroditsky, 2011).

Feel like you might only be getting Cat Burglar Barbie? Check other sources to see if they've "dressed" the facts differently (Doctor Barbie? Student-During-Midterms Barbie? Super-Talkative-Person-on-the-Bus Barbie?)

And Put Your Money Where Your Mouth Is!

Diversify your news sources; support sources offering critical thinking and reputable investigative reporting.

And do not share or re-tweet stories that appear suspect. Fake News needs to circulate in order to survive. You can stop it in its tracks.

Activity

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=75#h5p-3

Call out lies. Don't ignore them.

> "The point of challenging a lie is not to convince the liar, who is likely too far gone in his or her dark purpose to be rehabilitated. But because every lie has an audience, there may still be time to do some good for others."
>
> -Lee Mcintyre; *Post-Truth* (2018)

Withdraw your support from political candidates, organizations, or media outlets that share misinformation, disinformation, or fake news. The health of our information ecosystem, and of our democracies, relies on a public discourse based in truth.

> "Whether we call it post-truth or pre-truth, it is dangerous to ignore reality. And that is what we are talking about here. The danger of post-truth is not just that we allow our opinions and feelings to play a role in shaping what we think of as facts and truth, but that by doing so we take the risk of being estranged from reality itself."
>
> -Lee Mcintyre; *Post-Truth* (2018)


WARNING
FAKE NEWS

1. References

SARAH GIBBS

Above the Noise. (2017, May 3). *Why do our brains love fake news?* [Video]. YouTube, https://youtu.be/dNmwvntMF5A.

Above the Noise. (2019, June 12). *False equivalence: Why it's so dangerous* [Video]. YouTube, https://youtu.be/oFC-0FR2hko.

Bennett, W. & Livingston, S. (2020) Preface: The origins and importance of political disinformation. In W. Bennett & S. Livingston (Eds.), *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States* (pp. Xv-Xxv). Cambridge University Press. doi:10.1017/9781108914628.012

Common Sense Media Ratings & Reviews. (2017, January 31). *5 ways to spot fake news* [Video]. YouTube, https://youtu.be/g2AdkNH-kWA

Cooke, N.A. (2018). *Fake news and alternative facts: Information literacy in a post-truth era.* ALA Editions.

McIntyre, L. (2018). *Post-Truth*. MIT Press. MIT Press Essential Knowledge Series.

O'Connor, C. & Weatherall, J. O. (2019). *The misinformation age: How false beliefs spread.* Yale University Press.

Orlowski, J. (Director). (2020). *The Social Dilemma* [Film]. Netflix.

Orwell, G. (1945). Notes on nationalism. In S. Orwell & I. Angus (Eds.), *The Collected Essays, Journalism and Letters of George Orwell* (Vol. 3, pp. 361-380). Harcourt, Brace & World.

Orwell, G. (1946). The prevention of literature. In S. Orwell & I. Angus (Eds.), *The Collected Essays, Journalism and Letters of George Orwell* (Vol. 4, pp. 59-72). Harcourt, Brace & World.

Ovide, S. (2021a, May 28). Facebook takes on superspreaders. *The New York Times On Tech with Shira Ovide*. https://messaging-custom-newsletters.nytimes.com/template/oakv2?campaign_id=158&emc=edit_ot_20210528&instance_id=31815&nl=on-tech-with-shira-ovide&productCode=OT&regi_id=93354323&segment_id=59325&te=1&uri=nyt%3A%2F%2Fnewsletter%2F9549dc3d-4cb1-5629-95f0-6ac6df96d991&user_id=818c575cc91f8bf846ed0399d25a209f

Ovide, S. (2021b, June 22). The big impact of small changes. *The New York Times On Tech with Shira Ovide*. https://messaging-custom-newsletters.nytimes.com/template/oakv2?abVariantId=0&campaign_id=158&emc=edit_ot_20210622&instance_id=33585&nl=on-tech-with-shira-ovide&productCode=OT&regi_id=93354323&segment_id=61383&te=1&uri=nyt%3A%2F%2Fnewsletter%2Ffda60203-0708-535c-85dc-859a26c165b5&user_id=818c575cc91f8bf846ed039d25a209f

Rathje, S. (2017, July 20). The power of framing: It's not what you say, it's how you say it. *The Guardian.* https://www.theguardian.com/science/head-quarters/2017/jul/20/the-power-of-framing-its-not-what-you-say-its-how-you-say-it

Starr, P. (2020). The flooded zone: How we became more vulnerable to disinformation in the digital era. In W. Bennett & S. Livingston (Eds.), *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States* (pp. 67-92). Cambridge University Press. doi:10.1017/9781108914628.003

Stencel, M. & Luther, J. (2020, October 13). Fact-checking count tops 300 for the first time. *Duke Reporters' Lab.* https://reporterslab.org/fact-checking-count-tops-300-for-the-first-time/

Thibodeau P.H. & Boroditsky, L. (2011). Metaphors we think with:

The role of metaphor in reasoning. *PLoS ONE* 6(2): e16782, 1-11. https://doi.org/10.1371/journal.pone.0016782

PART II

PART II: DATA COMMODIFICATION & SURVEILLANCE

Figure 1.

Big Brother is Now Big Tech

Note. From Big Brother is now Big Tech [Digital Art], by Valery Brozhinsky, n.d-a., Shutterstock (https://tinyurl.com/h4cudd6y). Standard License.

2. 1: Introduction

ADRIAN CASTILLO

Our time is marked by an extreme reliance on digital technologies and the de facto privatization of the Internet; both have brought unprecedented advances in global communication and profound new challenges that are lessening trust, democratic stability, and social cooperation (United Nations, 2009). Under those circumstances, we must critically examine how digital technologies are increasingly facilitating the massive gathering, use, and monetization of personal data. How can we assert we are "digital citizens" if we are restricted to act as mere data producers under surveillance rather than data owners who have rights? In other words, how is the 21st century reshaping the understandings of citizenship we have brought with us from the 20th century?

With that in mind, the purpose of this section is to foster democratic attitudes that go beyond the primary teaching of digital skills related to online safety and privacy. The *Data commodification & surveillance* section will help learners establish themselves as active digital citizens who have the power to change the laws and norms of cyberspace and to evaluate how they contribute to the common good in the age of surveillance capitalism.

Learning Objectives

After finishing this chapter, readers will be able to:

1. Define "surveillance," "privacy," and "data

commodification."

2. Compare and contrast the positive and negative aspects of surveillance in different historical contexts.
3. Analyze the various arguments provided by groups in power to justify data commodification.
4. Identify digital platforms that foster data commodification and use the knowledge they have gained of platform structures and of privacy-protecting practices in order to resist data harvesting.

3. 2: Definitions

ADRIAN CASTILLO

Asking for the true meaning of a word involves inquiring about its context, that is, the other words around it. With that in mind, think about the words "surveillance" and "espionage"; they may appear identical in meaning–and although closely associated by negative undertones–they can be distinguished primarily by purpose and less by practice: *Surveillance* means "close watch kept over someone or something (as by a detective)." By contrast, *espionage* means "to watch secretly, usually for hostile purposes" (Merriam-Webster, n.d., para.2).

Beyond their literal and precise meanings (denotations), words suggest ideas and carry with them emotional associations that can be positive and negative, rarely neutral (connotations). Thus, the definitions below provide basic descriptions from the Oxford English Dictionary and examples grounded in real-life events courtesy of distinguished scholars. Both enable us to have a shared understanding of our subject; they allow us to find "true meaning."

Surveillance: the act of carefully keeping close watch over someone or something to gather information, influence, manage, or direct. The word originates in the early 19th century with French, *surveiller*, *sur-* 'over' + *veiller* 'watch' (from Latin *vigilare*': 'vigil watchful') (Oxford University Press, n.d.-a; Monahan & Wood, 2018). Choi-Fitzpatrick (2020) notes that current surveillance programs exploit technologies such as drones and satellites for negative and positive purposes (e.g. weaponized remote-control war, advancing climate change research).

Espionage: the process of secretly gathering confidential information using human sources (agents) or technical means (like hacking into computer systems) without permission from the source of information (Oxford University Press, n.d.-b; MI5, n.d.-a).

- **Interesting Fact #1:** In 2020, the Canadian Security Intelligence Service (CSIS) detected "espionage and foreign interference activity at levels not seen since the Cold War" (Tunney, 2021, para. 3). The target was usually non-governmental organizations, including academic institutions and private companies. Research and development firms, like biopharmaceutical companies involved in vaccine development (Tunney, 2021), were particularly targeted.
- **Interesting fact #2:** The English security service M15 explains that espionage can take many forms, including military (theft of defense capability intel), industrial (theft of trade secrets for economic gain), or political (theft of negotiating positions), and often supports efforts to sabotage politicians or influence decision-makers and opinion-holders (M15, n.d.-b).

Privacy: a person's right to keep matters secret and not be watched or disturbed by other people. In addition, privacy can be defined as freedom from unauthorized intrusion (Oxford English Dictionary, n.d.-c; The International Association of Privacy Professionals [IAPP], 2021). A related term is "information privacy," which can be defined as "the right to have control over how your personal information is collected, shared, and used" (IAPP, 2021).

- **Interesting fact #1:** Recognizing privacy as a human right depends largely on a particular country's laws and social and ethical norms. Therefore, a person's right to privacy varies widely according to the distribution of freedom and authority in different societies (Wenar, 2020). As an illustration, China rates as one of the worst abusers of internet freedom; according to Statista (2019), "censorship and surveillance [in the country] [have been] pushed to unprecedented extremes" (para.3). **How free is the Internet?** Governments worldwide differ considerably regarding internet access, limits to online content, and violations of user rights. To learn more, check this world map, courtesy of Statista (2019).

- **Interesting fact #2:** Can you have personal security without privacy? The simple answer is yes. Privacy and security are related concepts; however, you can have perfect security without privacy. Consider that security is only a technical method to protect your personal information, for example, antivirus software. On the other hand, privacy is a right safeguarded by laws and regulations that give you control over how, when, and by whom your information is used (Herzog, 2016). As a result, while security is necessary, it is not sufficient for enshrining privacy as a right (IAPP, 2021). Remember, becoming both private and secure is part of exercising your digital citizenship.

Data Commodification: the process of acquiring, storing, and treating often personal data like a product that can be bought and sold (Oxford University Press, n.d.-d). Examples include biometric and health-related data, as well as internet browsing patterns, click-through rates, geolocation coordinates, and other sensitive information.

- **Interesting Fact #1:** The five most valuable firms in the world today (Apple, Amazon, Facebook, Microsoft, and Google's parent company, Alphabet) are essentially data firms as, without data, these businesses could not operate or even generate any value (Sadowski, 2019).

4. 3: History

ADRIAN CASTILLO

Surveillance is a neutral-value concept that is as old as civilization itself. The basic idea of gathering information about individuals has been connected to sinister and good ends. Hence, on the one hand, surveillance can be associated with the subjugation of people or "disciplining the watched subjects" (Galic et al., 2017), as seen throughout history in colonialism, fascism, communism, and even within democratic societies when anti-democratic behavior is practiced (Marx, 2015). Conversely, surveillance has also been used for good ends and is fundamental for effective governance; this is exemplified in the provision of security, public health surveillance, or in any event where surveillance does not flow downwards or serves to disadvantage individuals (Marx, 2015).

Figure 2.

The School of Athens (Scuola di Atene)

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=111#h5p-7

Note. From *The School of Athens by* Raphael Sanzio (1511), Wikimedia Commons (https://tinyurl.com/3ycp7vhe). In the public domain.

Surveillance in Classical Greece (500-336 BC)

Although today we relate surveillance to the use of technology, early surveillance practices appeared in the cradle of Western civilization, namely, classical Greece. The culture from which ideas about modern democracy derive conceived surveillance as a

repressive and normalizing tool. As an illustration, Plato and Aristotle argued that careful official monitoring of the population was needed to control the lack of order that grew from the liberty to "do as you please" (Johnstone, 2003, p. 260). Aristotle even stated the following in his book series *Politics*:

[The ruler must] see to it that none of the things his subjects say or do escapes his notice; rather, he must have spies [Kataskopoi], . . . in any gathering or conference, for when men fear they speak less freely, and if they do speak freely they are less likely to escape notice" (as cited in Russell, 2000, p. 107).

Thus, we can see how surveillance was used as a tool for social conformity and erosion of intellectual freedom. On the other hand, Greek culture fostered a strong desire for honor (Johnstone, 2013) and thus a willingness to be subject to the judgment of others. Even the word honor is defined as "good name or public esteem" and is associated with reputation, merit, and recognition (Merriam-Webster, 2021, definition of honor section). As such, Greek democracy made explicit what was implicit, namely honor as a system of surveillance: "To win honor . . . a person must live his life in public" (as cited in Johnstone, 2013 p. 259).

Early surveillance practices collected information using interpersonal contact between people rather than technical means (Watson, 2021).

Surveillance in Nazi Germany (1933 – 1943)

Infamous for its brutality and racism, Nazi Germany created a form of political policing meant to maintain the status quo and eliminate all political dissidents (United States Holocaust Memorial Museum, 2021). The Gestapo, also known as the "Secret State Police," gathered information about the population by searching homes and apartments, reading suspects' mail, listening to telephone conversations, and applying brutal methods of interrogation.

Surveillance in the Soviet Union (1922-1991)

All ideological extremes have created their political policing forms; however, crucial differences in purpose, method, and

function have historically made the KGB notorious. According to Hein (2012), the KGB, the security agency of the Soviet Union, was primarily concerned about what people were *thinking*. Consequently, the agency created ideological re-education interrogations and lectures that boasted Soviet achievements. The Stanford historian Amir Weiner explains "[Soviet] interrogations aimed at reducing their targets to a state of utter helplessness, to the point that they realized the aimlessness of their previous existence and submitted to Soviet power or, even better, converted to its cause" (as cited in Hein, 2012, Mind control section).

Western colonialism and surveillance (1500 AD – the 1950s)

When colonial powers seized new territories, they used surveillance as a reformatory strategy, which commonly segregated the local Indigenous populations into isolated enclaves. For example, Smith (2009) notes that when Euro-Canadians imposed themselves in First Nations territory, they created "Indian reserves" limited not only by geographical borders but also cultural and racial barriers, whereby missionaries could indoctrinate Indigenous peoples into religious practices and social conducts acceptable to Euro-Canadians.

Following the rationale of surveillance as a reformatory strategy, the 1880s saw the creation of the Canadian Indian Residential School System, a colonial effort led by three institutions: the Canadian government, the Catholic Church, and various Protestant churches. The goal was to "[t]o civilize and Christianize" (The Truth and Reconciliation Commission of Canada [TRC], 2015, Preface section) and "[t]o kill the Indian in the child" (UBC First Nations and Indigenous Studies, 2017, para. 5). To achieve that, the residential school system broke the bonds between Indigenous parents and their children and, ultimately, sought to assimilate them into Canadian society (Historica Canada, n.d.; First Nations Education Steering Committee, 2017). The residential school system lasted until the closing decades of the 20th century. Its legacy is intergenerational trauma, loss of language, and death (TRC, 2015).

Eventually, the colonial models of surveillance that were once

exercised on colonized countries and subjugated peoples found their way back to Western governments and were used against their own peoples. The French philosopher, Michelle Foucault, identified this as "[t]he Imperial Boomerang Effect," which means "the West practicing something resembling colonization [...] [on] itself" (as cited in Berda, 2013, p. 629).

Surveillance in Liberal Democracies (Present)

A central feature of liberal democracies is their systems of checks and balances, which are intended, among other things, to prevent domestic security agencies from engaging in invasive surveillance practices **(**Hein, 2012). Nevertheless, in 2013, a former systems administrator for the CIA, Edward Snowden, made public how the U.S. National Security Agency (NSA) obtained direct access to servers of internet firms, including Facebook, Google, and Apple, in order to track online communication in a surveillance program known as Prism (Greenwald & MacAskill, 2013).

Under the Prism program, the NSA collected, without any warrants, the search history, the content of emails, file transfers, and live chats of millions of Americans (Greenwald & MacAskill, 2013)**.** Edward Snowden's actions as a whistleblower are now seen as pivotal to igniting a public debate on accountability, surveillance, and the role of public and private actors in administrating the internet.

More details about the NSA are explored in the following video:

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=111#h5p-34

The New York Times. (2013, November 4). *The NSA's evolution:*

Surveillance in a post-9/11 world [Video]. YouTube. https://www.youtube.com/watch?v=97C0mgQ6v6E

The following chapter examines a new kind of internet surveillance, this time for economic purposes.

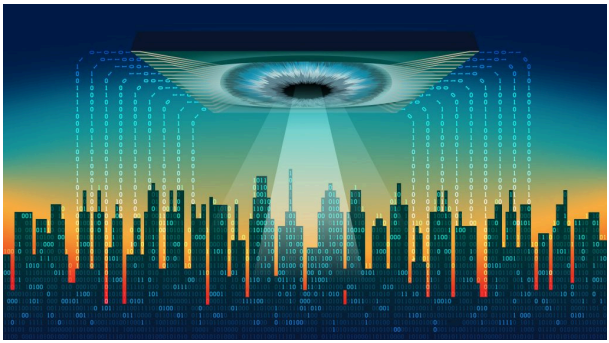
5. 4.1 The Rise of Surveillance Capitalism

ADRIAN CASTILLO

> "He thought of the telescreen with its never-sleeping ear. They could spy upon you night and day, but if you kept your head, you could still outwit them. With all their cleverness, they had never mastered the secret of finding out what another human being was thinking."
>
> —George Orwell, *Nineteen Eighty-Four* (1949)

Figure 3.

The Digital City & Big Brother.



Note. From The Digital City & Big Brother [Digital Image], by Valery Brozhinsky, n.d., Shutterstock (https://tinyurl.com/m76ytexr). Standard License.

Published 72 years ago, Orwell's dystopian novel, *Nineteen Eighty-*

Four, warned humanity about sinister technologies of mass surveillance, such as telescreens, devices that predicted our voice-activated speakers like *Alexa*, security cameras such as Google's video doorbell *Nest Hello*, and the microphones embedded in our smartphones, and combined them with our most sophisticated mass communication media, the television. Hence, telescreens can be described as omnipresent eyes, ears, and voices. The twenty-first century is blurring the lines between Orwell's dystopian fiction and reality. Today technological omnipresence (ubiquity) is accompanied by technological omnipotence (unlimited power), as our current technologies are "controlled by just five global mega-corporations that are bigger than most governments" (Pringle, 2017, para. 1), namely, Apple, Amazon, Facebook, Microsoft, and Google's parent company, Alphabet. Together, they are known as "Big Tech" or the "Big Five," and they are conglomerates whose power is threatening our freedom and democracy (Zuboff, 2019a).

It all began in the early 2000s when Google pioneered a new form of "interest-based advertising" (Finkelstein, 2009) called Google AdSense. According to Google, this is a simple way to earn money on publisher's websites by displaying ads that are automatically targeted to the site content and audience (Google, n.d., how AdSense works section). The explanation provided by Google, although simple, is not transparent since it does not explain how AdSense collects large amounts of personal data for marketing purposes. Let's see what information Google is tracking, according to Geary (2012):

- **time:** 06/Aug/2008 12:01:32
- **ad_placement_id:** 105
- **ad_id:** 1003
- **user id:** 0000000000000001
- **client_ip:** 123.45.67.89
- **referral_url:** "http://youtube.com/categories"

At first glance, that information may seem incomprehensible, but those pieces tell Google:

- **time:** the time and date you saw an advert.
- **ad_placement_id:** the ID of where the advert was seen on the site.
- **User id:** the unique ID number the cookie has given your browser.
- **Client_ip:** your country and town/city.
- **ad_id:** the unique ID of the advert.
- **referral_url:** what page you were on when you saw the advert.

That is how AdSense collects and scrutinizes our online behavior, but it doesn't stop there. The "Big Five" use similar practices. Apart from Google, Facebook has high-level systems for data collection, even data about people who have not signed on to the platform (Nielo, 2020). In other words, we believed Facebook predominately collected our status updates, photos, comments, and likes. On the contrary, for Facebook, the most critical information is what we don't consciously share with the platform: our browsing activities on millions of other websites (Azhar, 2019). The social platform does this by tracking users across the web and behind the scenes with a piece of code called "Facebook Pixel" (John, 2018). This code enables Facebook to know when you accessed a website, including date, time, URL, browser type, and other online behaviors. Then, Facebook can match that data with your Facebook profile and return a version of that data to the website owner. According to Facebook's VP for Public Policy, Richard Allan, "The cookies and pixels we use are industry standard technologies…" (as cited in Lomas, 2018, para. 5). In fact, cookies are used by 41% of all websites, of which 34.6% use non-secure cookies with unencrypted connections that could become be a security threat (W3Techs, 2021).

In response to the new realities of the internet, Shoshana Zuboff, former Harvard professor, philosopher, and scholar, coined the term

"surveillance capitalism." The term defines the economic system that hijacked the Internet and its digital technologies to commodify human experience and transformed it into data, with the core purpose of monitoring, influencing, and predicting human behavior, which can be analyzed and sold (Zuboff, 2019b).

Professor Zuboff explains "surveillance capitalism." Please watch.

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=133#h5p-13

The Lavin Agency Speakers Bureau. (2019, May 14). *What is surveillance capitalism?* [Video]. YouTube. https://www.youtube.com/watch?v=fwNYjshqZ10&t=1s

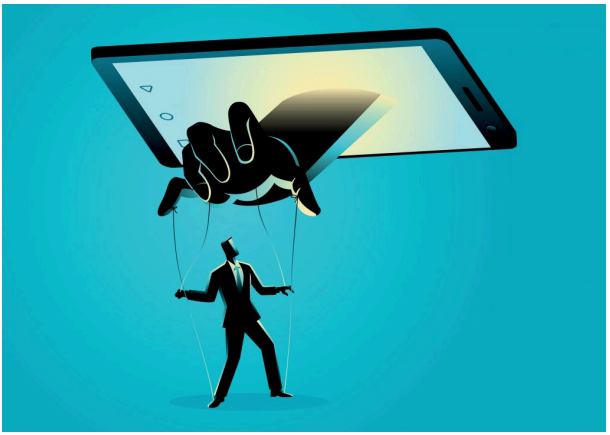
Nevertheless, Zuboff (2019b) clearly states that she is after "the puppet master, not the puppet" (p.30). In other words, surveillance capitalism is not a technology. It is the logic that commands technology to blend commercial goals with technological necessities. The scholar argues that Big Tech firms want people to think that surveillance practices are inevitable expressions of their digital technologies. For example, search engines do not store data, surveillance capitalism does (Zuboff, 2019a). According to Warren (2018), while you can delete your browser history, you won't be able to delete what is stored in Google's servers. Furthermore, we must not see digital technologies as tools pre-destined to steal our data, but rather as tools designed by people, artificially made, meticulously calculated. Therefore, we can change their nature through democratic legal regulation.

Big Tech: A Threat to Democracy?

"We can have democracy, or we can have a surveillance society, but we cannot have both" (Zuboff, 2021, para. 1).

Figure 4.

Smartphone control.



Note. From Smartphone controlling person. [Digital Image], by Rudall30, n.d., Shutterstock (https://tinyurl.com/46e9j67f). Standard License.

Back in 2018, the Cambridge Analytica scandal made headlines when it was revealed how the political research firm stole the Facebook data of millions of Americans before the 2016 election, intending to give Ted Cruz and Donald Trump's campaign big data tools to compete with Democrats (Detrow, 2018). Cambridge Analytica's wrongdoings came to light when whistleblower, Christopher Wylie, a Canadian data analytics expert who worked for the firm, told the press: "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on" (as cited in Cadwalladr & Graham-Harrison, 2018a, para. 3).

To gather data from Facebook users, Cambridge Analytica used an app called *this is your digital life*; it featured a personality quiz

that recorded the data not only of each person taking the quiz, but crucially, extracted the data of that person's Facebook friends as well (Cadwalladr & Graham-Harrison, 2018b). As a result, Cambridge Analytica obtained massive datasets that allowed the firm to build personality profiles and segment American voters into categories, such as: "high in conscientiousness and neuroticism," or "high in extroversion but low in openness," among other traits (Wade, 2018). Next, the segmentation was used to tailor highly individualized political messages and misinformation campaigns on topics related to immigration, the economy, and gun rights (Wade, 2018).

All of these actions were completed without the knowledge or consent of the American electorate (Cadwalladr, 2019). Consequently, Zuboff (2019b) explains that Cambridge Analytica is the perfect illustration of surveillance capitalism's tactical approach and its ultimate purpose: "[Surveillance capitalism was] designed to produce ignorance through secrecy and careful evasion of individual awareness" (p. 303).

These events prompted Canadian scholar Taylor Owen (2017) to analyze if Facebook threatens the integrity of Canadian democracy. The scholar explains that Facebook is a potent political weapon, which by means of consumer surveillance and customized information feeds (micro-targeting), can allow buyers such as foreign actors, companies, or politicians to purchase an audience. This scheme may facilitate buyers "to define audiences in racist, bigoted and otherwise highly discriminatory ways" (para. 4). In addition, Owen (2017) explains that even without Facebook's micro-targeting, much of its content is not accessed for quality or truthfulness, and can therefore manipulate huge audiences with low-quality clickbait information.

The Cambridge Analytica Presentation: A Misleading Pitch?

"I don't get it. Why are they confessing?"

> "They're not confessing. They're bragging."
> – *The Big Short* (2015)

Infamous for manipulating American voters, today Cambridge Analytica has dissolved; however, before the firms' scandal made headlines, Cambridge Analytica's CEO, Alexander Nix, was happy to share in a conference how the firm harvested Facebook data from a survey undertaken by "hundreds" of Americans. Nix explains the survey data allowed his firm to "form a model to predict the personalities of every single adult in the United States of America" (Concordia, 2016, 3:42). In addition, Nix describes how the company used psychographic targeting to influence votes through customized messages, including "fear-based messages" (Concordia, 2016, 4:20). Thus, we can say that Alexander Nix exemplifies the very definition of a surveillance capitalist.

Please watch the videos below and answer their respective Google Form questions. The questions are open-ended and there are no wrong answers! Just elaborate your ideas as much as you can. Most importantly, your answers are anonymous and will be used exclusively to improve the content of the present eBook.

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=133#h5p-33

[devXnull]. (2018, April 25). *CEO Alexander Nix speaks about Cambridge Analytica* [Video]. YouTube. https://www.youtube.com/watch?v=UaS8LksPHJs

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://openeducationalberta.ca/digitalcitizenship/?p=133#h5p-14

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://openeducationalberta.ca/digitalcitizenship/?p=133#h5p-16

CBC News. (2018, March 19). *Canadian whistleblower Christopher Wylie talks about Cambridge Analytica* [Video]. YouTube. https://www.youtube.com/watch?v=MuFRg-CU6Nc

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://openeducationalberta.ca/digitalcitizenship/?p=133#h5p-15

At its core, Facebook is a political tool because we live in the information age. As Zuboff (2021) explains in a recent *New York Times* article:

> In an information civilization, societies are defined by questions of knowledge — how it is distributed, the authority that governs its distribution, and the power that protects that authority. Who knows? Who decides who

> knows? Who decides who decides who knows? Surveillance capitalists now hold the answers to each question, though we never elected them to govern. This is the essence of the epistemic coup. They claim the authority to decide who knows by asserting ownership rights over our personal information and defend that authority with the power to control critical information systems and infrastructures. (para. 3)

From Online to Onlife

"Technology has outmatched our brains, diminishing our capacity to address the world's most pressing challenges. The advertising business model built on exploiting this mismatch has created the attention economy. In return, we get the 'free' downgrading of humanity" (Harris, 2019, para. 17).

Figure 5.

Social Media may lead to non-substance addiction.

Note. From Social Media may lead to non-substance addiction. [Digital Image], by Overearth, n.d., ShutterStock (https://tinyurl.com/27p54t36). Standard License.

In the post-industrial information age, Zuboff argues that the cause

of our digital issues is the accumulation of economic and knowledge power in the hands of big tech. Conversely, a former design ethicist at Google, Tristan Harris, argues that the source of our problems is how business models in technology seek to exploit our minds, more precisely our limited attention spans. According to Harris (2019), even if we fixed the privacy issues whereby big tech firms collect and monetize from our personal data, we would still have to face the fact that our technology can easily outmatch our brains (i.e. our addiction to online social validation, our love for "likes, our obsession with scrolling through news feeds"). They would all persist and carry on with destroying our attention spans. Indeed, in a recent survey across Canada, over 75% of respondents indicated that they spend "at least 3-4 hours online every day, and 15 percent are spending more than eight hours online per day" (Canadian Internet Registration Authority, 2020).

Back in 2013, Harris made a 141-slide deck entitled A *Call to Minimize Distraction & Respect Users' Attention*, in which he explains his goal is to create a new design ethic that aims to minimize distraction; otherwise, Harris explains, our technologies will systematically worsen our human shortcomings, including:

- **"Bad Forecasting"** (a.k.a. "that won't take long") Harris (2013) illustrated that humans are bad at estimating how long a task is going to take. For example, in a Facebook notification alerting you that you had been tagged in a photo, the label would say something like "see your photo." Harris suggests the label should read "spend next 20 minutes on Facebook" (slide, 46). Thus, Harris recommends that technology should help users forecast the consequences of certain actions, so they can make informed decisions.
- **"Intermittent variable rewards"'** (a.k.a. slot machines) Just like playing in a casino, Harris (2013) suggests that intermittent rewards are the hardest to stop, and easily become addictive. As an illustration, we constantly refresh an app like Twitter or Facebook to find "reward" in new content.

- **"Loss aversion** (a.k.a. "the fear of missing out") Harris (2013) states that what is stopping us from turning off our alerts or phone notifications is the fear of missing an important event. We think that at any moment we could receive a message saying "Hey, a nuclear bomb just exploded over your house" (slide, 67). Harris says we should have the option to disconnect.
- **"Fast and slow thinking"** (a.k.a. Mindful vs Mindless behavior) According to Harris (2013), people make different decisions when they have time to pause and reflect vs when they react impulsively. If technology is made "too frictionless" we stop thinking (e.g. when scrolling is frictionless we can flick for hours). Harris (2013) suggests creating "speed bumps" that provide us time to think.
- **"Stress and altered states"** (a.k.a. "I am not in the best state of mind to decide") Finally, the tech ethicist warns us that technology is affecting our overall health through anticipation of alerts, which creates stress, and a cascade effect of physiological responses. Overall, these human vulnerabilities enable big tech to steal our time.

Although Zuboff and Harris may disagree on what is cause and what is consequence (economic system vs. human psychology), both arrive at the same conclusion: big tech has become a threat to human agency and wellbeing.

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=133#h5p-17

Terms of Service: Click to Agree with What?

> "However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization." – Amazon's Terms of Service, Section 42.10

Terms of Service are the legal agreements or "contracts" between a service provider and the person who wants that service (LePan, 2020). The great majority of people do not read these unescapable online "contracts," and there is a good reason for that.

Figure 6.

Drowning in paperwork.

Note. From Drowning in Paperwork. [Digital Image], by Photobank Gallery, n.d., Shutterstock (https://tinyurl.com/4wfuhxca). Standard License.

According to LePan, (2020), the average person would need almost 250 hours to read all digital contracts properly. Likewise, Zuboff (2019b) states that many websites push users to agree with terms of service just for browsing a website. In addition, many terms of service can be modified by service providers unilaterally at any time, without user awareness. To make things worse, terms of service typically involve other companies and third parties. Zuboff (2019b) explains that a recent study by academics from the University of London shows that to enter the ecosystem of Google's smart home devices (Nest Home), users may need to read a thousand contracts. LePan (2000) offers the following table calculating how much time it would take to read the terms of services different companies provide (according to their word count and based on a reading speed of 240 words per minute):

Table 1

Terms of service reading time

App/Service	Word Count	How many minutes to read? (240 wpm)
Microsoft	15,260	63.5
Spotify	8,600	35.8
Niantic (Pokemon Go)	8,466	35.2
TikTok	7,459	31.4
Apple (Media Services)	7,314	30.5
Zoom	6,891	28.7
Tinder	6,215	25.9
Slack	5,782	24.1
Uber	5,658	23.6
Twitter	5,633	23.5

Note. The table shows App/ Services beginning with the largest word counts. Table is taken from LePan (2020).

Consequently, we can see how terms of services place a heavy reading load on consumers. Terms of service are voluminous, non-negotiable documents; by design, they don't encourage any scrutiny. As an illustration, imagine having to read 50-printed pages when entering a bowling alley, which is the equivalent of Microsoft's 15,000-word terms of service.

Activity Time!

1. Please visit the website "Terms of Service. Didn't Read." It will provide you with summaries of companies' terms of service, and an overall rating of their quality from the user's standpoint.
2. Identify a company or service to which you already subscribe.
3. Based on the summaries from "Terms of Service. Didn't Read," follow the instructions in the Google Form

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://openeducationalberta.ca/digitalcitizenship/?p=133#h5p-18

As we have seen in this section, surveillance capitalism is a potentially dangerous economic logic. In the next chapter, we will learn some tactics to counter surveillance capitalism.

6. 4.2 What to do: Tactics to Counter Surveillance Capitalism

ADRIAN CASTILLO

> "If the soul is left in darkness, sins will be committed. The guilty one is not he who commits the sin, but the one who causes the darkness."
> — Victor Hugo, *Les Misérables* (1862)

Figure 7.
Data fist

Note. From Data Fist [Digital Image], by Valery Brozhinsky, n.d., Shutterstock (https://tinyurl.com/u53kbvap). Standard License.

The quotation from Victor Hugo suggests how social structures (such as education, religion, or political institutions) are decisive in shaping individual behavior, and can both constrain or expand a person's agency (the ability to exercise free will and make choices) (Gibbs, 2017). There is an ongoing debate on how to best counter surveillance capitalism: while many scholars argue that we should focus on strengthening political institutions through offensive measures, such as developing laws and compulsory models for data governance, privacy rights, and the prevention of monopolies (Geist, 2020; Micheli et al., 2020; Owen, 2019), other experts

suggest that we should focus on learning defensive measures, using our agency to study encryption and other privacy tools, reclaiming personal data stored in platform companies, or developing ethical online behaviors (Mattson, 2021; Ribble & Park, 2019).

While it is true that focusing only on defensive measures would leave surveillance capitalism intact, it is also true that we can and should use our agency to learn about the benefits and risks of specific digital technologies. Thus, this section will provide strategies to counter surveillance capitalism through offensive measures (emphasis on structures) and defensive measures (emphasis on personal agency).

A story of Defensive Measures: Paul-Olivier Dehaye

"I have made mistakes. The biggest one was to go it alone. Without allies you can't win these sorts of conflicts" (as cited in *The Local*, 2018).

Paul-Olivier Dehaye is a Belgian mathematician and data ownership activist, who in December 2016, emailed Facebook asking for the profile data the company harvested with the code Facebook Pixel., explained in the video below.

Please watch:

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=287#h5p-19

CBC News. (2018, April 11). *Facebook, advertisers and your data explained* [Video]. YouTube. https://www.youtube.com/watch?v=daoCwHARvGo

Even though as a Belgian citizen, Dehaye was protected by the European Union's Charter of Fundamental Rights, "whose privacy laws are considered the global gold standard" (*The Economist*, 2018, para. 1). It took Facebook 106 days to answer his email, explaining the company couldn't fulfill his request in its totality.

After another maze of emails that lasted over a year, Facebook clarified that Dehaye's data was stored in *Hive*, Facebook's data storage for data analytics. Facebook stated that it would take a disproportionate effort to retrieve that data. Hive's data is "also not used to directly serve the live Facebook website which users experience" (as cited in Zuboff, 2019b, p. 688). In other words, Facebook was saying that because it was too difficult to find its users' complete data, the company deserved to be above the law (Martineau, 2018). In reality, Hive's data is Facebook's exclusive realm in which behavioral data is stored to manufacture prediction products (Zuboff, 2019b). Eventually, Facebook dismissed Dehaye's complaint, due to a lack of enforcement of data laws by the Irish Data Protection Commissioner, which Dehaye's calls "the biggest [Facebook] enabler" (Dehaye, 2018, para.9). Despite this, the mathematician was able to have a hearing in the European Parliament, which made his case widely known. Dehaye's case exemplifies the possibilities and limits of agency from the "bottom-up" (Micheli et al., 2020).

Activity #1

How to find out what Facebook knows about you.

Following on Dehaye's footsteps, let's figure what data is Facebook willing to provide about each of us. To do this, watch the video below, then log into your Facebook profile and follow these instructions to download a copy of your Facebook data.

*Due to time constraints, download only data from the last three months.

The download should take anywhere from **five-to-ten minutes**,

depending on the amount of data you are downloading. Therefore, continue reading through this section, then come back to answer the questions below.

Please watch the video below and answer the Google Form questions. Please remember, the questions are open-ended and there are no wrong answers! Just elaborate your ideas as much as you can. As explained in previous chapters, your answers are anonymous and will be used exclusively to improve the content of the present eBook.

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=287#h5p-20

CNN Business. (2018, March 27). *How to find out what Facebook knows about you* [Video]. YouTube. https://www.youtube.com/watch?v=9EKGmNa9jAA

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=287#h5p-21

Understanding Browser Tracking

Every time we use the internet we leave a footprint on the websites we have visited. There are many techniques to follow our online

movements; however, one of the most popular ways is embedding a small piece of data into our web browsers–this is known as a **cookie.** Cookies are designed to "store registration data, to customize information for visitors to a website, to target online advertising, and to keep track of the products a user wishes to order online" (Britannica, 2017, para. 1).

We can further understand website tracking with the video below. Please watch:

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=287#h5p-22

[GCFLearnFree.org]. (2017, September 8). *Understanding digital tracking* [Video]. YouTube. https://www.youtube.com/watch?v=6EHSlhnE6Ck

Note that cookies are *designed*, which means that we could also create an alternative web experience in which privacy is "proactive, not reactive; preventative not remedial" (Cavoukian, 2011, the 7 foundational principles section). This is known as *Privacy by Design* (PbD), the main advantage is that it prevents privacy-invasive risks from occurring, as privacy is embedded into the architecture of IT systems; it is not an add-on (Cavoukian, 2011).

Privacy Applications that you Can Trust:

Since defensive measures are important in our digital era, you can enhance your privacy by downloading many privacy-related applications on the website PrivacyTools. The website is trustworthy since it does not utilize paid recommendations or affiliate programs that are very common elsewhere online.

In addition, we can examine how some Canadian news websites, unfortunately, employ extensive tracking practices. Please open

Trackography. This site offers a visualization tracker guide and includes the tracking practices of many popular news outlets, including *The National Post*, *The Calgary Herald*, or *The Toronto Sun*. Similarly, you can find global news outlets, such as CNN, BBC, or *El Pais*. Moreover, Trackography shows countries around the world hosting the servers where their websites store our tracked data.

Offensive Measures: Governing Data as Oil or Sunlight?

As technology corporations such as Google and Facebook continue to grow, governments are catching up by imposing legislation to limit their power and enhance accountability. An example of this is Canada's Digital Charter, which is trying to establish practices that protect our personal information in the private sector (Government of Canada, 2021a). The *Digital Charter Implementation Act* promises to build a "foundation of trust and transparency between citizens, companies, and government" (Government of Canada, 2020, para. 5). The legislation will ensure that Canadians are protected in the modern data-driven economy. It mandates:

- **Meaningful Consent:** Increases control and transparency in online consent rules, mandating they are written in plain language, so people can make informed choices on how companies handle their personal information.
- **Data Mobility**: Allows Canadians to direct the transfer of personal information between organizations in a secure manner. For example, individuals can tell a bank to transfer or share their data with another financial institution.
- **Disposal of personal information and withdrawal of consent:** Ensures that Canadians can demand an organization to destroy their information. It also permits the withdraw of consent for the use of personal information.

- **Algorithmic transparency:** Empowers Canadians to request clarification on how companies apply automated decision-making systems like algorithms and artificial intelligence in making predictions, recommendations or decisions about individuals.
- **De-identified information:** ensures the privacy of Canadians by removing any identifiers (such as name) in information disclosed without consent.

At its core, the *Digital Charter Implementation Act* recognizes the tension between personal data as a right, and personal data as a commodity. A means to understand this tension is available in the question "Are data more like oil or sunlight?" (*The Economist*, 2020). The question emphasizes that data can be extracted, tagged, and sold (just like oil); however, unlike oil, data is a renewable source, just like solar rays, which are free, are everywhere and cover everything.

The metaphor is further explored in the video below. Please answer the Google Form question after watching.

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=287#h5p-23

[FT Rethink]. (2018, November 1). *Is data the new oil?* [Video]. YouTube. https://www.youtube.com/watch?v=kG-Naum0Dvk

An interactive H5P element has been excluded from this

version of the text. You can view it online here:
https://openeducationalberta.ca/
digitalcitizenship/?p=287#h5p-24

As we have seen, there are a number of perspectives on how to best counter surveillance capitalism, the economic logic that turns all aspects of our life into digital data, all human nature into ones and zeros. In the next chapter, we will consider our Datafied society.

7. 5. Datafication, Dataism, and Dataveillance

ADRIAN CASTILLO

> "[Machine learning models] can evaluate a person better than the average work colleague, merely on the basis of ten Facebook 'likes.' Seventy 'likes' were enough to outdo what a person's friends knew, 150 what their parents knew, and 300 'likes' what their partner knew. More 'likes' could even surpass what a person thought they knew about themselves"
>
> – Michal Kosinski, *Tech by Vice* (as cited in Grassegger & Krogeous, 2017)

Figure 8.

The Face of Big Data

Note. From The Face of Big Data [Digital Image], by Pink Eyes, n.d., Shutterstock (https://tinyurl.com/5btumanw). Standard License.

In the twenty-first century, the explosion of available data is reshaping our economy and reconfiguring human culture, and eventually, it will transform human nature (Zuboff, 2019b). As big tech encourages people to move their social interactions into digital environments, language is beginning to change.

Think about the words "friending" and "liking." Both define relations mediated by algorithms. Or the words "followers" and "retweet." The former defines an online persona through popularity, and the latter the amplification of a thought (Van Dijck, 2014). As a result, participating in digital environments risks turning the language of friendship, which is based on reciprocity and affirmation, into industry-driven language, which quantifies social relations (number of likes, shares, followers, etc) that can be easily mined and repurposed into "precious products" (Van Dijck, 2014, p. 199). The influence that technology has over our lives goes beyond the confines of language, however. Technology is rendering human experiences into data that has never been quantified before; this is a phenomenon called "datafication" (Cukier and Mayer-Schoenberger, 2013).

With that in mind, it is important to clarify that the engine driving datafication is not only our digital interactions but the massive amounts of data we can process, which is known as "Big Data" (Cukier and Mayer-Schoenberger, 2013). Big data helps answer what, not why, due to its hierarchical nature (data, information, knowledge, wisdom) (Strasser and Edwards, 2017). To shed light on that hierarchy, data can be seen as raw material, often unorganized numerical facts which, when organized and combined within a specific context or set of relations, becomes information. In turn, information helps us to create meaning that when brought together with experience assists in decision-making processes, resulting in knowledge. Consequently, the life-long accumulation of knowledge, and crucially, the experience of failure, when examined provides wisdom, which is the "capacity to choose objectives consistent with one's values within a larger societal context" (Logan, 2014, p.44). Because information is a refinement of basic data, there are huge

efforts to transform big data into something humanly comprehensible; these efforts have traditionally included data visualization and machine learning (Mani, 2020).

The following video examines how we use big data and machine learning algorithms in real life:

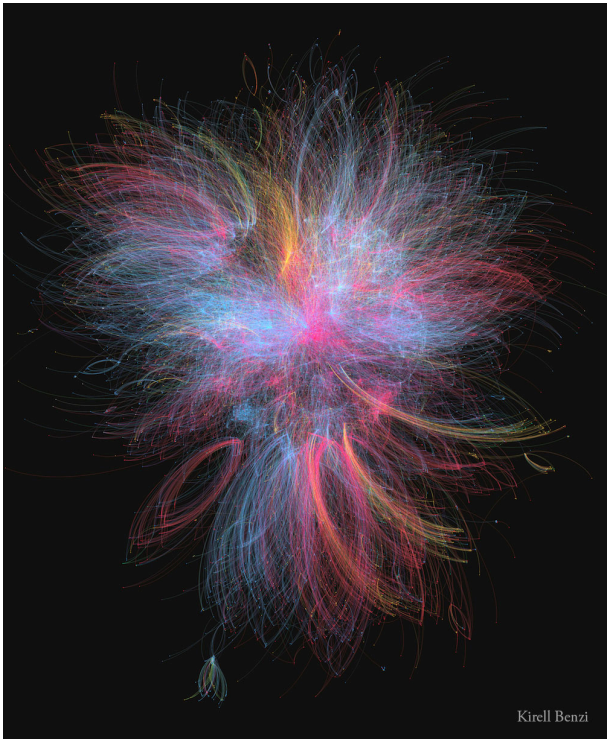
> *An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=311#h5p-35*

Open Society Foundations. (2016, December 13). *Life in a quantified society* [Video]. YouTube. https://www.youtube.com/watch?v=UemXBXgawKY

Data visualization can help us understand Big Data patterns, like in figure # 9, created by the Ph.D. in Data Science and data artist, Dr. Kirell Benzi; the visualization shows how over 20.000 different Star Wars characters connect through their storylines (Benzi 2015):

Figure 9.

The Dark Side and The Light Side



Note. From The Dark Side and The Light [Network Art], by Kirell Benzi, 2015 (https://www.kirellbenzi.com/art/dark-side-light). Copyright 2015 by Kirell Benzi. Reproduced with permission.

According to Benzi (2015):

- **blue nodes:** represent all the factions associated with the light side of the Force (Jedis, The Republic, The Rebellion).
- **Red nodes**: represent all the factions associated with the dark side of the force (the Siths and the Empire)
- **Yellow nodes:** represent all the factions related to bounty hunters and criminals.

Obviously, big data can also help with other issues like understanding the history of pandemics.

As we have seen in previous chapters, data is collected by close observation (surveillance). It is important to remember that

surveillance is a neutral-value concept. Therefore, it can be used for good or ill. The following section describes the combination of data and surveillance practices into what is called "dataveillance."

The Better Angels of Surveillance and Data (a.k.a. Dataveillance):

It is vital to point out the ethical complexities of surveillance and data activities. Arguably, all these practices or tools can be used for positive as well as sinister ends, *welfare* as well as *warfare*. The only pre-condition is that they act as servants of democracy, not its masters, which requires the vigilant eyes of educated digital citizens and their political representatives. Here are a few ways in which surveillance and data can be used for our welfare:

The Quantified-Self: the term refers to the culture of self-tracking through wearable technologies, especially technologies focused on improving sleep, diet, and health in the name of greater efficiency (Grinberg, 2019). There are a variety of views about this practice. On one side of the argument, Grinberg (2019) explains that self-tracking follows a neoliberal conception of the self as a business unit. In other words, life is constructed as a balance sheet, which is made evident in the administrative vocabulary of the self-tracking culture (e.g. annual, monthly, or weekly reports, budgets, and balances). On the other hand, Sharon and Zanderberg (2016) argue that the quantified-self movement is being attacked based on prejudice that labels individuals as narcissistic. On the contrary, the authors suggest how self-tracking goes beyond wearable sensors and is characterized by positive practices, such as *self-tracking as a mindfulness practice.* For example, learning to grieve through a digital spreadsheet that logs memories of the lost person.

COVID-19 Data and Surveillance: Public health departments routinely monitor, collect, and analyze people with certain illnesses or infections. This process is known as "case surveillance" (Centers

for Disease Control and Prevention, 2021). During the COVID-19 pandemic, the Public Health Agency of Canada has been using case surveillance with the primary goal of containing the pandemic and lessening the damaging health effects of the virus on Canadians. Case surveillance has also been used to find new evidence on the epidemiological features of the disease (Government of Canada, 2021b).

As stated in previous chapters, surveillance capitalism is not a technology; it is an economic logic centered on profit-making. When this logic is turned upside down, our mobile devices become valuable for public health officials, who managed to stop 400 chains of infection in Canada as of May 2021 (Daigle & Zimonjic, 2021). Officials deployed the *COVID Alert app*, the federal government's app designed to exchange the Bluetooth signals of phones to notify users when they have been in contact with someone who tested positive so that they can isolate (Daigle & Zimonjic, 2021).

Big Data in Cancer Research: In medicine, "big data" refers to the mass acquisition of patient records, including patient characteristics, diagnostic and treatment history, and billing accounts (Tsai et al., 2019). In cancer research, big data has the potential to detect cancers sooner (allowing for earlier intervention), assess unique risk factors, and even identify connections between genetic, environmental, and socioeconomic factors (Canadian Cancer Research Alliance, 2020).

Dataism: A New Religion?

The comprehensive enumeration of the world into data is leading to a new paradigm called *Dataism*, which is a new mindset or philosophy, where value and wisdom reside in data and its analysis, leaving aside experience and human intuition (Lohr, 2015). Dataism is a concept popularized by many journalists and scholars, but most notably, Dr. Yuval Harari, who is a historian, scholar, and

best-selling author. The video below further explains what dataism is, please watch:

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=311#h5p-26

University of California Television. (2019, February 23). "*Listen to Google" from theism to humanism to data-ism* [Video]. YouTube. https://www.youtube.com/watch?v=Hw2jBiqZ4N8

An interactive H5P element has been excluded from this version of the text. You can view it online here: https://openeducationalberta.ca/digitalcitizenship/?p=311#h5p-27

In conclusion, in the Internet era, surveillance and datafication, although prevalent, need not define our future. It is in our hands to become digital citizens who own our data and decide when it is appropriate to share it.

8. References

ADRIAN CASTILLO

Azhar, H. (2019, June 26). Politicians Don't Trust Facebook—Unless They're Campaigning. *Wired*. https://tinyurl.com/3hv9czx8

Benzi, K. (2015). *The Dark Side and The Light Side* [Network Art]. https://www.kirellbenzi.com/art/dark-side-light

Berda, Y. (2013). Managing dangerous populations: Colonial legacies of security and Surveillance. *Sociological Forum*, *28*(3), 627–630. https://doi.org/10.1111/socf.12042

Britannica. (2017). Cookie. In *Encyclopedia Britannica*. Retrieved August 1, 2021 from https://www.britannica.com/topic/cookie-electronic-monitoring

Britannica. (2021). Great Purge. In *Encyclopedia Britannica*. Retrieved August 1, 2021 from https://www.britannica.com/event/Great-Purge

Brozhinsky, V. (n.d.-a). *Big brother is now big tech* [digital art]. Shutterstock. https://tinyurl.com/h4cudd6y

Brozhinsky, V. (n.d.-b). *The digital city & big Brother* [digital art]. Shutterstock. https://tinyurl.com/m76ytexr

Cadwalladr, C., & Graham-Harrison, E. (2018a, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://tinyurl.com/jjfxpvr9

Cadwalladr, C., & Graham-Harrison, E. (2018b, March 17). How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool. *The Guardian*. https://tinyurl.com/6c3yw963

Cadwalladr, C. (2019, March 17). Cambridge Analytica a year on: 'a lesson in institutional failure'. *The Guardian*. https://tinyurl.com/42pf8mun

Canadian Cancer Research Alliance. (2020). *Cancer research: Big data and precision health*. https://bit.ly/3i5SDX3

Canadian Internet Registration Authority. (2020). *Canada's internet fact book. https://tinyurl.com/24ppcanu*

Cartwright, M. (2020). Warfare in Classical Greece. In *World History Encyclopedia.* Retrieved July 26, 2021 from https://bit.ly/3xhvs0x

Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles.* https://tinyurl.com/464zvf7r

Centers for Disease Control and Prevention. (2021). *FAQ: COVID-19 data and surveillance.* https://tinyurl.com/vmuxztap

Choi-Fitzpatrick, A. (2020). *The good drone : How social movements democratize surveillance.* MIT Press.

Concordia. (2016). *Cambridge analytica – The power of big data and psychographics* [Video]. YouTube. https://tinyurl.com/veyj8rd2

Cukier, K., Mayer-Schoenberg, M. (2013). The Rise of Big Data. *Foreign Affairs*, https://tinyurl.com/2758zay6

Daigle, T. & Zimonjic, P. (2021). *Federal COVID Alert app caught 400 cases of COVID-19 in April.* CBC News. https://bit.ly/3zD1ghQ

Dehaye, P. O. (2018). *Testimony at european parliament.* https://tinyurl.com/9ddznc3k

Detrow, S. (2018). *What did Cambridge Analytica do during the 2016 election?*. NPR. https://n.pr/378WDzI

Finkelstein, S. (2009, March 26). Google's surveillance is taking us further down the road to hell. *The Guardian.* https://bit.ly/3iXD1nI

First Nations Education Steering Committee. (2017). *Grade 11 / 12 Indian Residential Schools and Reconciliation.* https://bit.ly/3i2sDMi

Galič, M., Timan, T. & Koops, B. (2017). An overview of surveillance theories from the panopticon to participation. *Philos Technol.* 30**,** 9–37. https://doi.org/10.1007/s13347-016-0219-1

Geary, J. (2012, April 23). Doubleclick (Google): What is it and what does it do?. *The Guardian.* https://tinyurl.com/7zw65x9v

Geist, M. (2020). *Canada's GDPR moment: Why the consumer privacy protection act is Canada's biggest privacy overhaul in decades.* https://bit.ly/35jjBU6

Gibbs, B. J. (2017). Structuration theory. In *Encyclopedia Britannica.* Retrieved August 1, 2021, from https://www.britannica.com/topic/structuration-theory

Grassegger, H., Krogeous, M. (2017). *The data that turned the world upside down.* Tech by Vice. https://tinyurl.com/c7t24hye

Greenwald, G. & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian.* https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Google. (n.d.). *How AdSense works.* AdSense Help. https://tinyurl.com/tcvc73md

Government of Canada. (2020). *Fact Sheet: Digital Charter Implementation Act.* https://tinyurl.com/378us3jf

Government of Canada. (2021a). *Canada's digital charter: Trust in a digital world.* https://tinyurl.com/5byft7fj

Government of Canada. (2021b). *National surveillance for Coronavirus disease (COVID-19).* https://bit.ly/37dvFqB

Grinberg, Y. (2019). Sensored: *The quantified self, self-Tracking, and the limits of digital transparency* [Doctoral Dissertation, Columbia University]. Columbia Academic Commons. https://academiccommons.columbia.edu/doi/10.7916/D8N604CK

Harris. (2013). *A call to minimize distraction and respect users' attention* [PowerPoint slides]. http://www.minimizedistraction.com

Harris, T. (2019, December 5). Our brains are no match for our technology. *The New York Times.* https://tinyurl.com/3shdfae3

Hein, B. (2012). *Getting to know you: Stanford scholar examines domestic surveillance in the USSR.* Stanford News.

https://news.stanford.edu/news/2012/october/kgb-domestic-surveillance-100212.html

Herzog. (2016). *You can't have privacy without security*. National Cyber Security Alliance. https://bit.ly/3rzNKc5

Historica Canada. (n.d.). *Residential schools in Canada: Education guide*. https://bit.ly/3eVp9t5

Hugo, V., & Buffum, D. L. (1908). *Les misérables*. Henry Holt and Co.

John, A. (2018). *How Facebook tracks you, even when you're not on Facebook*. Consumer Reports. https://tinyurl.com/edpnwecc

Johnstone, S. (2003). Women, property, and surveillance in classical Athens. *Classical Antiquity*. , *22*(2), 247-274. https://doi.org/10.1525/ca.2003.22.2.247

Kulwin, N. (2019, February 24). Shoshana Zuboff on surveillance capitalism's threat to democracy. *Intelligencer*. https://tinyurl.com/f4sep23z

LePan, N. (2020). *Visualizing the length of the fine print, for 14 popular apps*. Visual Capitalist. https://bit.ly/3xbvUNN

Logan, R. (2014). *What is information? Propagating organization in the biosphere, symbolosphere, technosphere and econosphere* [PDF]. https://tinyurl.com/5bmmwfwu

Lomas, A. (2018). *Facebook's tracking of non-users ruled illegal again*. Tech Crunch. https://tcrn.ch/3i8sHtO

Lohr, S. (2015). *Data-ism: The revolution transforming decision making, consumer behavior, and almost everything else*. HarperCollins.

Mani, C. (2020, October 20). How Is Big Data Analytics Using Machine Learning?. *Forbes*. https://tinyurl.com/nbf573h6

Marx, G. T. (2015). Surveillance Studies. In J. D. Wright (Ed.), *International encyclopedia of the social & behavioral sciences* (Vol. 23, pp. 733–741). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Martineau, P. (2018). *Zuckerberg's testimony contradicted his own privacy ops team*. https://tinyurl.com/x486a7z4'

Mattson, K. (2021). *Ethics in a digital world: Guiding students through society's biggest questions*. International Society for Technology in Education.

Merriam-Webster. (2021). Honor. In *Merriam-Webster.com dictionary*. Retrieved July 25, 2021 from https://www.merriam-webster.com/dictionary/honor

Merriam-Webster. (n.d.). Trending surveillance. In *Merriam-Webster.com dictionary*. Retrieved July 26, 2021 from https://bit.ly/3BLQnfB

Micheli, M., Ponti, M., Craglia, M., & Berti-Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*. https://doi.org/10.1177/2053951720948087

MI5. (n.d.-a). *Counter-espionage*. Security Service MI5. https://bit.ly/3BK0P7m

MI5. (n.d.-b). *Targets of espionage*. Security Service MI5. https://bit.ly/3rFe8Bo

Monahan, T., & Wood, D. M. (2018). *Surveillance studies: A reader*. Oxford University Press.

Nielo, D. (2020, January 12). All the ways Facebook tracks you–and how to limit it. *Wired.* https://tinyurl.com/54we47p8

Nishiyama, H. (2020). Racializing surveillance through language: the role of selective translation in the promotion of public vigilance against migrants. *Ethnic and Racial Studies*, 43(10), 1757-1775. https://doi.org/10.1080/01419870.2019.1654115

Orwell, G. (1949). *Nineteen Eighty-Four.* Penguin Classics.

Overearth. (n.d.). *Social Media may lead to non-substance addiction* [Digital Image]. Shutterstock. https://tinyurl.com/27p54t36

Owen, T. (2017, October 19). Is Facebook a threat to democracy?. *The Globe and Mail.* https://tgam.ca/2V2xOD7

Owen, T. (2019). *The case for platform governance* [PDF]. Centre for International Governance Innovation. https://bit.ly/3sqr8KI

Oxford University Press. (n.d.-a). Surveillance. In *Oxford learner's Dictionaries*. Retrieved July 26, 2021 from https://bit.ly/3x7MTjG

Oxford University Press. (n.d.-b). Espionage. In *Oxford Learner's Dictionaries*. Retrieved July 26, 2021 from https://bit.ly/2UQet8d

Oxford University Press. (n.d.-c). Privacy. In *Oxford Learner's Dictionaries*. Retrieved July 26, 2021 from https://bit.ly/3zvFht8

Oxford University Press. (n.d.-d). Commodity. In *Oxford Learner's Dictionaries*. https://bit.ly/3i2hefs

Parenti, C. (2004). *The soft cage: Surveillance in America from slavery to the war on terror*. Basic Books.

Photobank Gallery. (n.d.). *Drowning in Paperwork* [Digital Image]. Shutterstock. https://tinyurl.com/4wfuhxca

Pink Eyes. (n.d.). *The Face of Big Data* [Digital art]. Shutterstock. https://tinyurl.com/5btumanw

Pringle, R. (2017). *'Data is the new oil': Your personal information is now the world's most valuable commodity*. CBC News. https://bit.ly/3x3O97L

Ribble, M., & Park, M. (2019). *The digital citizenship handbook for school leaders: Fostering positive interactions online*. International Society for Technology in Education.

Rudall30. (n.d.). *From Smartphone controlling person* [digital art]. Shutterstock. https://tinyurl.com/46e9j67f

Russell, F. S. (2000). *Information gathering in classical Greece*. University of Michigan Press.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, 6(1). 1-12. https://doi.org/10.1177/2053951718820549

Sanzio, R. (1511). *The School of Athens* [painting]. Wikimedia Commons. https://tinyurl.com/3ycp7vhe

Sharon, T., & Zandbergen, D. (2016). From data fetishism to quantifying selves: Self-tracking practices and the other values of data. *New Media & Society*, 19(11), 1695–1709. doi:10.1177/1461444816636090

Smith, K. D. (2009). *Liberalism, surveillance, and resistance: Indigenous communities in western Canada*. AU Press.

Statista. (2019). *How free is the internet?*. https://bit.ly/3ic5mI1

Strasser, B. J., & Edwards, P. N. (2017). Big data is the answer…

but what is the question? *Osiris*, 32(1). 328-345.https://doi.org/10.1086/694223

The Economist. (2018). *The EU guarantees its citizens' data rights, in theory*. https://tinyurl.com/jh9ekpse

The Economist. (2020). *Are data more like oil or sunlight?*. https://tinyurl.com/6tp73cau

The Editors of Encyclopaedia Britannica (2019). Anthropometry. *In Encyclopedia Britannica.* Retrieved July 26, 2021 from https://bit.ly/3eZDzbM

The International Association of Privacy Professionals. (2021). *What does privacy mean?*. IAPP. https://bit.ly/3y9PAma

The Local. (2018). *How a Swiss-based mathematician helped lift the lid on the Facebook data scandal.* https://tinyurl.com/kxpmjru7

Truth and Reconciliation Commission of Canada. (2015). *Honouring the truth, reconciling for the future: summary of the final report of the truth and reconciliation commission of Canada.* Truth and Reconciliation Commission of Canada. https://bit.ly/3BGetIF

Tsai, C. J., Riaz, N., & Gomez, S. L. (2019). Big data in cancer research: real-world resources for precision oncology to improve cancer care delivery. *Seminars in Radiation Oncology*, *29*(4), 306–310. https://doi.org/10.1016/j.semradonc.2019.05.002

Tunney. (2021). *CSIS says 2020 was a banner year for espionage operations targeting Canada.* CBC News. https://bit.ly/37hzTxP

UBC First Nations and Indigenous Studies. (2017). *The Residential School System*. Indigenous Foundations. https://bit.ly/3BOfRJk

United Nations. (2019). *The age of digital independence* [PDF]. Report of the United Nations Secretary-General's High-Level Panel on Digital Cooperation. https://bit.ly/2UTYtSH

United States Holocaust Memorial Museum. (2021). *The Gestapo: Overview.* https://encyclopedia.ushmm.org/content/en/article/gestapo

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data

between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. https://bit.ly/3i4uuk1

Wade, M. R. (2018). *Psychographics: the behavioural analysis that helped Cambridge Analytica know voters' minds.* Real Learning, Real Impact. https://tinyurl.com/629wn5j9

Watson, B. W. (2012). Intelligence. In *Encyclopedia Britannica*. Retrieved July 26, 2021 from https://bit.ly/3zJmt9Z

Warren, T. (2018). *Google is making it easier to wipe out your search history.* The Verge. https://bit.ly/3xbL4Ck

Wenar, L. (2020). Rights. In E. N. Zalta (Ed), *The Stanford Encyclopedia of Philosophy*. Retrieved July 26, 2021 from https://stanford.io/3i5TirD

Wylie, C. (2019, October 4). How I Helped Hack Democracy. *Intelligencer*. https://tinyurl.com/54fyx4bw

W3Techs. (2021). *Usage statistics of non-secure cookies for websites.* https://tinyurl.com/xkcsckxy

Zuboff, S. (2019a, June 6). The surveillance threat Is not what Orwell imagined. *Time*. https://bit.ly/2VhOCGd

Zuboff, S. (2019b). *The age of surveillance capitalism*. Profile Books.

Zuboff, S. (2021, January 29). The coup we are not talking about. *The New York Times*. https://nyti.ms/2WqDQOd