‘THEOS’

Data and Dignity

Why Privacy Matters in the Digital Age

Nathan Mladin

‘THEOS’

Theos is the UK’s leading religion and society think tank. It has a broad Christian basis and exists to enrich the conversation about the role of faith in society through research, events, and media commentary.

Images: from Pexels.com and shutterstock.com

Published by Theos in 2023

Images: from Pexels.com and shutterstock.com

Theos Licence Department
77 Great Peter Street
London SW1P 2EZ

+44 (0) 20 7828 7777
hello@theosthinktank.co.uk
theosthinktank.co.uk

Data and Dignity

Why Privacy Matters in the Digital Age

Nathan Mladin

This essay in one minute

It's becoming old news: we are continually tracked, analysed, and profiled by private companies and governmental agencies. Our data is hoovered up and used to predict and manipulate our behaviour. Indeed, the use of big data and algorithmic systems is on the rise in our world. A new cultural and economic order is here: surveillance capitalism or what this essay calls the "surveillance system".

The first three chapters of the essay describe this system, looking at social media, facial recognition, and predictive policing.

Of the many concerns raised, privacy is never far from the top. But what is privacy? Most often, it is seen as an individual's right to control their data. But this is not enough. If it is to serve us well in resisting dehumanising applications of technology, privacy must be re-imagined around a truer, more rounded view of what it means to be human.

Drawing on Christian thought – though anticipating overlap with other religious and philosophical traditions – the second half of the essay sketches a conception of privacy rooted in the notion of dignity and based on the sort of creatures human beings are: *embodied* (with limits and susceptibilities to be honoured rather than violated for gain); *relational* (made for relationships of trust and mutual care rather than exploitation); *agential* (with a capacity for intentional action to be upheld rather than undermined).

Privacy is not dead, nor should it be allowed to die. Privacy is a form of neighbour love in the digital age.

Contents

Introduction

You know that BASH has over 40 million data points on you, on every decision you have made since 1994, Doctor? I know when you have colon polyps months before your doctor does... Much, much more importantly than that, I know what you are. I know who you are... You think you're motivated by beliefs, high ethical beliefs, but you just run towards pleasure and away from pain like a field mouse. Our algorithms can even predict how you'll die to 96... 96.5% accuracy. Your death was so unremarkable and boring I can't remember the details apart from one thing. You're gonna die alone.

– Don't Look Up (Netflix, 2021)

This is what Sir Peter Isherwell, the sinister tech mogul from Netflix's popular political satire *Don't Look Up* (2021), says to Dr Mandy, the astronomer trying to tell the world that planet earth is bound for destruction after an inevitable impact with a comet. Although fictional, what is chilling about this scene is how plausibly close Isherwell's brag – about the size of his data sets, the power of his algorithms, and the precision of his predictions – is to real life today.

While the conversation about Artificial General Intelligence (AGI)[1] (a hypothetical technological tipping point when computers radically exceed human capabilities and, on some readings, even become conscious) rumbles on, a stealthier but no less potent form of artificial intelligence, in the form of machine learning models and other algorithmic systems, is taking hold in our world. It is shaping everything, from our shopping experiences, entertainment consumption, relationships, to sectors such as financial services, human resources, policing, and social services, in decisive and often deleterious ways.

The phenomenon is rightly generating interest from, among others, academics, civil rights and advocacy groups, and regulators. It has risen in public awareness in the aftermath of the Cambridge Analytica-Facebook scandal (about data-driven manipulation of election behaviour (2016).[2] More recently, interest in the topic can be seen in the popularity of the Netflix docu-drama *The Social Dilemma,* which was viewed by more than 38 million people in just four weeks after it was launched in 2020.

But what are the salient issues at stake in these seemingly technical matters? How (and why) have experts and wider society responded? And what are the deeper currents and concerns underlying such debates?

The issues that I focus on in this essay fall broadly within what Harvard emerita professor Shoshana Zuboff calls "surveillance capitalism", also known as the data or information economy[3], focused on pervasive harvesting and analysis of data for the purpose of generating monetisable predictions about individuals.[4] But the phenomenon I am seeking to describe, and which I prefer to call the "surveillance system", is not merely an economic or technological one. Indeed, technology is never free-floating but always socially, economically, and politically embedded, and therefore produces real-world effects (e.g. algorithmic decision-making systems deployed in education, policing, healthcare, which can contribute to entrenching discrimination and deepening inequalities). Moreover, technology is morally freighted rather than neutral. It always brings with it an implicit vision of the human and the good, and exerts a significant but often subtle shaping influence on those who interact with it.

> **Technology is morally freighted rather than neutral. It always brings with it an implicit vision of the human and the good, and exerts a significant but often subtle shaping influence on those who interact with it.**

[1] Also known as “true AI” or “full AI”. The terms are often used interchangeably.

[2] See the Netflix documentary *The Great Hack* (2019).

[3] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019).

[4] Shoshana Zuboff, “You Are the Object of a Secret Extraction Operation”, *The New York Times*, 12 November 2021, https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html?fbclid=IwAR0sKVlu4aoB874Cy3mLD8bhAIK-ErkZjX-gce9a3_01_6bbZSx-lst4TM8

Aims and structure

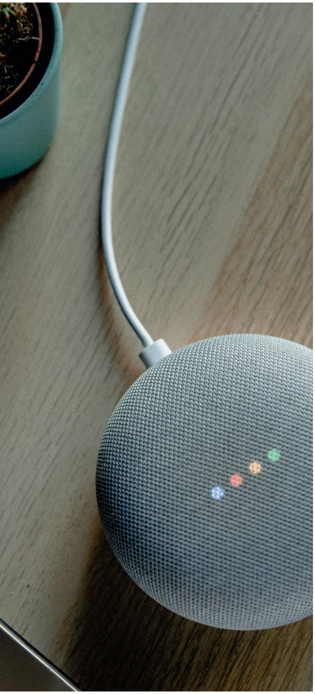
The first chapter describes what is going on at the intersection of data, algorithms, individuals, and society. Chapters 2 and 3 provide an analysis of what is at stake and review some of the key social and political consequences of social media, facial recognition technology, and so-called predictive or data-driven policing.

> Privacy is a basic human and social good and an ingredient in flourishing as the sort of creatures human beings are: *relational, embodied, agential* (i.e. with agency) creatures made for flourishing in relationships of trust. Protection of privacy should be seen as a form of neighbourly love in digital times.

In Chapter 4 I home in on the question of informational or data privacy. Indeed, invasion of privacy is one of the key issues raised about our increasingly data-driven societies. My thesis is that privacy is not dead, nor should it be allowed to die. But if it is to serve us well in resisting the dehumanising and depersonalising uses of technology that are proliferating today in our world, privacy must be re-imagined around a better, truer understanding of what it means to be human. Drawing explicitly on Christian thought – though anticipating overlap with other religious and philosophical traditions – I sketch a conception of privacy centred on the notion of dignity. Privacy, I argue, is not simply an individual right that attaches to an idealised autonomous individual. This is a short-sighted and deficient view.[1] Rather, privacy is a basic human and social good and an ingredient in flourishing as the sort of creatures human beings are: *relational*, *embodied*, *agential* (i.e. with agency) creatures made for flourishing in relationships of trust. Protection of privacy should be seen as a form of neighbourly love in digital times. The purpose of this essay is therefore to offer a wider anthropological and ethical foundation for reflecting on, and responding to, the concerns, harms, and injustices that arise in a world where data and algorithms play a significant and growing role. Before exploring this further, however, we must get a handle on what is going on.

[1] See Chapters 1 and 2 of Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge, UK: Cambridge University Press, 2018), pp. 13-33.

1
The surveillance system



It is becoming increasingly clear that we are embedded within systems that continually collect, analyse, and use our data to, among other things, manipulate our behaviour, particularly our choices as consumers through targeted advertising, and to grant or deny us access to essential products and services based on algorithmically determined profiling. We are constantly being surveilled – not by individuals working on behalf of authoritarian states, as was the case in communist Eastern European countries. Rather, we are the focus of powerful machines that work on behalf of private companies in the pursuit of profit. That said, state surveillance is similarly extensive and facilitated by the tight, if rather opaque, partnership that exists between tech companies and governmental agencies. Edward Snowden's revelations about the NSA and Wikileaks illustrate this well.

A surveillance business model is characteristic primarily of Meta (the parent company of Facebook, Instagram, and WhatsApp) and Alphabet (the parent company of Google, DeepMind, Calico, and other subsidiaries), as well as Chinese-owned social media companies TikTok and WeChat. However, the practice of surveillance is widespread and on the increase in the rest of the digital economy, in the public sector as much as in the private.

> “
>
> **Surveillance is widespread and on the increase in the the digital economy, in the public sector as much as in the private.**

In the engine room of the surveillance system are vast data sets ("Big Data") and powerful algorithmic systems such as machine learning models. Machine learning algorithms are cutting edge technologies "trained" on manually inputted data (often enormous data sets) to "learn" the correlations within the data sets and establish patterns. The trained algorithm, known as a machine learning model, can then automate future decisions. Increasingly, however, we are coming to realise that data sets are often flawed, contain biases, and reflect existing inequalities. Used as inputs for machine learning models, and in the absence of careful scrutiny, they perpetuate and reinforce those biases. In Virginia Eubanks' terms, they end up "automating inequality".[1] For example, Google shows ads for higher paid jobs to men and not women; image searches for "CEO" massively underrepresent women.[2] Or, to take an even more egregious example, a system designed to help treat up to 70 million US citizens in hospitals by allocating supplementary medical support for those with chronic illnesses was prioritising White patients over sicker Black patients.[3]

Today, at an AI-based company like Meta, engineers generate countless models with slight variations to see which one performs best.[4] Design ethicist and tech entrepreneur Tristan Harris famously describes this system in *The Social Dilemma* as a system that collects data in order to create something like a voodoo doll version of any one user. It then relentlessly tests which piece of content (usually ads) will grab attention and lead to "engagement". This happens in split seconds, as powerful machines are pointed at us with nearly every bit of information that is curated and pushed our way on social platforms.

There are six core parts to the surveillance system. (1) First, there is the extensive tracking of individuals across devices, apps, websites, social networks. With the spread of "smart" devices, ranging from TVs to toasters, tracking now also happens across the physical world as well.

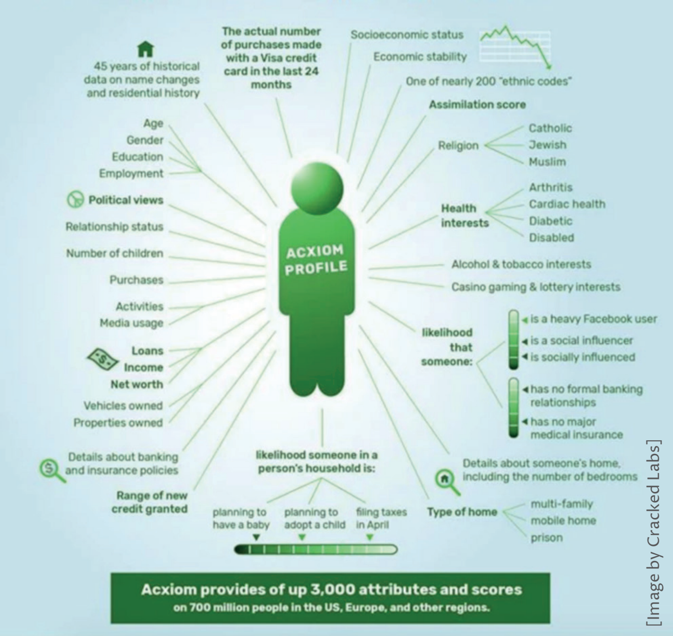
The purpose of this extensive surveillance apparatus is to collect as much data as possible. Meta does not simply collect data directly from their user's use of their platforms, but tracks them across the web using a piece of code known as Meta Pixel which records things like what other pages we see, what we purchase, and relates it back to Meta.

Simply carrying a smart phone, looking up places on Google Maps, hovering over TikTok videos, having an Amazon Echo or Google Dot device in one's house, or using wearable technology such as FitBit (owned by Alphabet), we are continually and unavoidably ceding data about ourselves: where we are, who we are with, our physical condition, our emotional state, and so on. Moreover, "smart" doorbells such as Amazon's Ring, enable an additional level of surveillance and targeting, as data, not just about ourselves or immediate family, but other individuals, flow surreptitiously towards various third parties in the private and public sector (e.g. law enforcement). The circulation and use of such data is generally opaque and unaccountable. Data from Ring devices, to take one example, is known to end up in the hands of law enforcement agencies without owners of the device having any awareness let alone say about it.[5]

The data collected from any one individual or household (e.g. “smart” TVs or “smart” electricity meters) is (2) aggregated with the data from billions of others in vast data sets (Big Data). The aggregated data is (3) extensively analysed using cutting-edge AI technology (i.e. machine learning algorithms or models), which perform a variety of statistical operations on the data sets.

These high-precision analytics (4) generate inferences and predictions about users and their behaviour. The detailed profiles and prediction analytics (not, generally, user data as such) are then (5) sold on to various third parties, primarily advertisers, but also banks, prospective employers, insurers etc. This is done through an opaque network of companies in the business of compiling, buying, and selling such detailed profiles and predictions. They are known as “data brokers” and include Experian, the credit score company, Acxiom, LexisNexis, among others.[6]

In 2017, data broker Acxiom provided up to 3,000 attributes on 700 million people. In 2018, the number was 10,000, on 2.5 billion consumers.


45 years of historical data on name changes and residential history
The actual number of purchases made with a Visa credit card in the last 24 months
Socioeconomic status
Economic stability
One of nearly 200 "ethnic codes"
Assimilation score
Age
Gender
Education
Employment
Religion
Catholic
Jewish
Muslim
Political views
Arthritis
Cardiac health
Diabetic
Disabled
Health interests
Relationship status
Number of children
ACXIOM PROFILE
Purchases
Alcohol & tobacco interests
Casino gaming & lottery interests
Activities
Media usage
likelihood that someone:
is a heavy Facebook user
is a social influencer
is socially influenced
Loans
Income
Net worth
has no formal banking relationships
has no major medical insurance
Vehicles owned
Properties owned
Details about banking and insurance policies
likelihood someone in a person's household is:
Details about someone's home, including the number of bedrooms
Range of new credit granted
planning to have a baby
planning to adopt a child
filing taxes in April
Type of home
multi-family
mobile home
prison
Acxiom provides of up 3,000 attributes and scores
on 700 million people in the US, Europe, and other regions.

[Image by Cracked Labs]

(6) Advertisers and other third parties (e.g. political parties, law enforcement agencies) use this information to reach people with targeted ads and condition people's behaviour or enact algorithmically determined decisions, for example in accessing personal loans, screening job candidates[7], or identifying criminals and administering justice and rehabilitation.[8] Indeed, data-fuelled algorithms do everything today from assigning work (e.g. Uber, Bolt, Deliveroo), curating our social media

feeds (e.g. Facebook and Twitter), to determining the potential partners we date or marry (e.g. Bumble, Tinder), and the products we are encouraged to buy (e.g. Amazon, Google).[9] These operations are generally opaque, given algorithms often operate as a "black box", and poorly scrutinised by relevant governance and regulatory bodies.

Data: donated, traded, or stolen?

There is no neutral way to talk about the role of data in our technologically driven societies and the relationship between people, data, and the organisations which handle it. Choice of language inescapably reflects philosophical and ideological commitments (e.g. pro/anti free-market capitalism, different conceptions of the human person, the nature of freedom which they enjoy etc.). While some speak of "donating" or "trading" their data for "free" products and services, this language presupposes an idealised conception of the human person. Much like the homo economicus of classical economic theory, it reflects an overconfidence in the rationality and agency of human persons, failing to account for non-rational factors that explain human decisions and actions and, at a more basic level, the fragility and finitude of persons – all of which can be manipulated and exploited more easily than we would like to admit.[10] This is why people like Shoshana Zuboff and Carissa Véliz prefer to describe the process as one of data "extraction", highlighting the marked asymmetry of power and knowledge between individual persons and the organisations who collect data, as well as the opaqueness maintained with regards to the use of data.

But data "extraction" may also be inaccurate language since it denies the agency of individuals, however limited and conditioned, as well as the indifference to data harvesting practices that many people show because they appreciate the benefits they receive (i.e. personalised content, including relevant ads, a powerful search engine, easy access to various services etc.).

Perhaps, then, a better way of describing the process is to refer to two dynamics: a casual acquiescence in data harvesting practices as well as manipulative co-option into said practices. However, as noted above, this turns on the anthropology employed in the analysis – the conception of the human person, and specifically our freedom, or lack of, to resist data collection, analysis, and algorithmically determined decisions.

The power of prediction

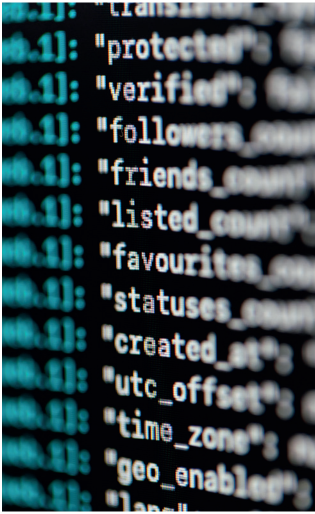
The capacity of algorithms to infer individual features and personal characteristics is staggering. Geolocation data, social media data, search history data, and so many other components of our Big Data trails can be highly revealing in the aggregate. For example, data from accelerometers – sensors fitted in almost all mobile devices and wearables – alone can indicate the location, health condition, gender, age, body features, emotional state, life expectancy, social interactions, and physical activities (e.g. writing, smoking, sorting through papers) of the device holder.[11]

In a study from 2015, researchers developed a model which can identify an individual's personality traits simply based on Facebook "Likes". The accuracy of the model surpasses that of the people who were close to the individual and knew him/her very well.[12] Big Data sets and machine learning allow tech companies to statistically predict a wide range of personal characteristics beyond what people willingly disclose on their social media profiles or through the content they generate.

> **Big Data sets and machine learning allow tech companies to statistically predict a wide range of personal characteristics beyond what people willingly disclose on their social media profiles or through the content they generate.**

Factors like gender, age, and political orientation, but also more granular information such as history of drug use, parental separation, sexual orientation, and mental health conditions, can all be inferred from Big Data sets.[13] For example, it takes a mere 68 Facebook "Likes", of any kind, to predict alcohol consumption, sexual orientation, mental health conditions. This holds even if the "Likes" do not map on to these criteria.[14] For Instagram users, models applied to the data extracted can diagnose depression based on elements like brightness, the number of faces and filters used in images uploaded to the platform. Similarly, computer models can predict real-life outcomes and other traits better than human judges.[15]

This kind of knowledge is derived from the vast troves of data collected across multiple platforms, websites, and devices and media, from billions of largely unaware users. The predictions, which are sold through an opaque network of third parties, including data brokers, to advertisers, governmental agencies, and other companies who employ data-powered predictions and analytics, are not based exclusively on the



```
.1]: "protecte
.1]: "verifie
.1]: "follower
.1]: "friends_
.1]: "listed_
.1]: "favourites
.1]: "statuses_
.1]: "created_at"
.1]: "utc_offset"
.1]: "time_zone"
.1]: "geo_enable
```

data that any one particular user yields. Rather they result from aggregated data to which an individual's personal data is only a small fraction. In other words, knowledge about any one person is derived not simply from the information they yield through their interaction with any given platform, device, or app, but from billions of other data points and the psychological and social profiling used to interpret it.

This explains the extensive knowledge that results and the power that accrues to it: to predict and, given its breadth and scale, ultimately to manipulate behaviour, especially in the case of targeted ads based on finely tuned profiles of "users". This is gravely concerning given the stark asymmetry of knowledge and power that exists between individuals and the entities who possess them. The whole business is decidedly non-relational. Put simply, we are known by impersonal corporate and state actors, with the help of powerful machines, but lack meaningful power to confirm or correct the knowledge derived about us and scrutinise the actions that such knowledge enables, whether we are the subject of those actions or others.

> "
>
> **We are known by impersonal corporate and state actors, but lack meaningful power to confirm or correct the knowledge derived about us and scrutinise the actions that such knowledge enables, whether we are the subject of those actions or others.**

Why concern about surveillance is lukewarm

Concern about the expansion of the surveillance culture and an increasing reliance on algorithms, what philosopher John Danaher calls "algocracy",[16] is on the rise. This is particularly the case in academic circles and the activist quarters of civil society. But a general outcry is nevertheless missing. Most people are happy to go along, unaware or indifferent to what elite analysts are describing with urgency. There are at least three factors to account for this situation: *lack of understanding* about the workings of the surveillance system and the life cycle of data; our love of *convenience* and the many affordances of digital technology; and our strong desire for *recognition and control*, which arguably underpin much of our activity on social media and our use of "smart" and self-monitoring devices.

Lack of understanding

Most people lack the technical knowledge about the workings of algorithms and how data are generated, extracted, analysed, and acted upon. Moreover, they do not feel the data they generate is in any meaningful sense theirs or related in any significant way to their personhood. This is particularly true of seemingly anodyne metadata, or data about data, such as call logs, information about what operating system or browser one is using, and so on. In itself, metadata feels removed from our personhood and sense of self, but in fact is highly revelatory when aggregated and analysed by powerful AIs. In the case of the owners and operators of algorithmically powered machines and systems, for example an insurance or credit scoring company, this is coupled with a naïve belief in the objectivity and neutrality of data and computation machines, in what is known as "the AI Halo Effect". Individual users of digital technology, as Robert Elliott Smith explains, "believe the results served up to us in online lists and searches are a true reflection of the world and the choices available to us therein. Numbers don't lie, and since machines just process numbers, neither can they."[17]

Convenience

Instant audio-visual communication afforded by social networks or the convenience of shopping in Amazon's one-stop-shop are tangible goods many value above more abstract goods such as privacy and "algorithmic justice" (except in situations when the absence of the latter are felt directly and personally). Plus, many are content to trade privacy for convenience or security. Whether they understand the full implications of forfeiting privacy, particularly those that manifest in the wider digital ecosystem and beyond what they might experience directly, is another matter (here, lack of understanding may also be a factor).

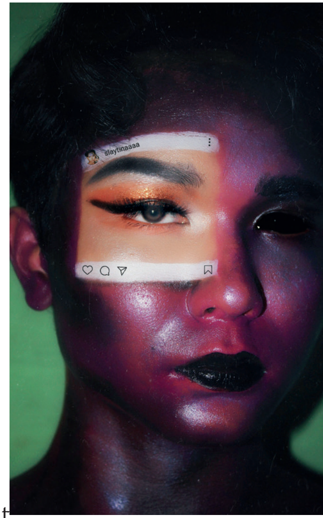
Criticisms of the products and services which people deem to have added considerably to their life satisfaction – say, keeping in touch with family and friends or using a powerful tool such as Google Maps – are perceived as attacks on the very benefits people genuinely cherish. Many struggle to understand that to criticise Facebook or Google, which run on an advertising-based extractive business model, is not to be against any form of social media, which allows for meaningful connection and communication, or digital products that genuinely add value and contribute to human flourishing. It is simply a refusal to accept that "there is no alternative" to surveillance capitalism.[18]

Desire for control and recognition

We are arguably inconsistent in our reactions to the surveillance system and conflicted about digital privacy in particular. This is because digital technology and digitally mediated relationships and experiences play off two of our fundamental desires: *to be seen or recognised*,[19] and *to control*.

Social media uniquely offers the possibility both to display oneself, often in carefully curated ways, to be seen and receive social recognition and approval, even if, for many, this proves to be fool’s gold at best, and poison at worst. Many of us have taken to displaying parts of our lives that would have been strictly demarcated as private. Social media and the proliferation of digital technology, within the constraints and incentives structure of capitalism, strongly encourage a blurring of boundaries between public and private, between online and offline living.

> **Digital technology and digitally mediated relationships and experiences play off two of our fundamental desires: to be *seen* or *recognised*, and to *control*.**



We also seem to have a love and hate relationship with control. The dominant view of privacy today is one of control over one’s data. But this is the case mostly among privacy experts and activists. The reality is that it is precisely out of a desire to manage, and ultimately control, one’s mental, physical, emotional, and spiritual health, that ordinary people relinquish privacy. We are seeing a rise in the desire and the capabilities to control. Testament to this are the variety of self-tracking fitness, wellbeing, and spirituality apps that together add up to what sociologists describe as the “quantified self” phenomenon and reveal what cultural commentator Alan Jacobs describes as the “psychological internalization of the impulse toward efficiency and productivity” which sits at the root of modern and late modern culture.[20] At the same time, fatigued by the proliferation of things to control and choices to make, we cede control or acquiesce in practices which erode it.

On a more speculative and philosophical note, the desire for control, which much digital technology caters to, is perhaps correlated with growing anxiety about the future, given a deepening climate crisis and its expected ramifications, political turmoil etc. Overarching narratives about the origin and direction of life, including hopeful visions about the future, have collapsed in our late modern age. The collapse of narratives of transcendent futures is met with a marked fixation on the present. "All we have is now" is the sentiment of the day. This perhaps explains the collective allergy to risk in our culture. All risk is to be eliminated. The extent to which this can be realised (although it is worth remembering complete elimination of risk is strictly impossible) depends on the level of power and agency one has. The more of these we have, the more we are able to eliminate risk.

A general aversion to risk and growing appetite for control is the deepest ambition both for the purveyors of surveillance technologies and "users". This is rooted in the conception of the person as autonomous, which is perfectly encapsulated by the concluding lines of the poem "Invictus" by William Ernest Henley: "I am the master of my fate, I am the captain of my soul". But if current trends in data collection, analysis, commercialisation are worrying, we need, as Chapter 4 of this essay will seek to show, a wider anthropological and ethical basis for both diagnosis and action – one that is not tethered to a conception of the human as an autonomous individual. But first we turn to outline some of the key social and political consequences of the surveillance system as they play out in relation to social media.

[1] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (London: Picador, 2019). See also Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (London: Penguin, 2017).

[2] Tom Simonite, "Probing the Dark Side of Google's Ad-Targeting System", *MIT Technology Review*, 6 July 2015, https://www.technologyreview.com/2015/07/06/110198/probing-the-dark-side-of-googles-ad-targeting-system/

[3] Madhumita Murgia, "The Franciscan monk helping the Vatican take on — and tame — AI", *Financial Times*, 7 April 2022, https://www.ft.com/content/1fa17d8b-5902-4aff-a69d-419b96722c83

[4] Karen Hao, "How Facebook got addicted to spreading misinformation", *MIT Technology Review*, 11 March 2021, https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/

[5] Matt Burgess, "All the Data Amazon's Ring Cameras Collect About You", *Wired*, 5 August 2022, https://www.wired.co.uk/article/ring-doorbell-camera-amazon-privacy

[6] Justin Sherman, "Big Data May Not Know Your Name. But It Knows Everything Else", *Wired*, 19 December 2021, https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/

[7] See "Computer Says No", a BBC documentary released on 16 March 2022 to raise awareness of the issue of AI recruitment and redundancy: https://www.bbc.co.uk/iplayer/episode/m0015gvw/computer-says-no

[8] "Algorithms in the Criminal Justice System", a report by The Law Society Commission on the Use of Algorithms in the Justice System and The Law Society of England and Wales, 4 June 2019, https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report

[9] Robert Elliott Smith, *Rage Inside the Machine: The Prejudice of Algorithms, and How to Stop the Internet Making Bigots of Us All* (London: Bloomsbury, 2019), Kindle version, 2%.

[10] Nathan Mladin, "The Social Dilemma and the Human Question", *Theos*, 23 September 2020, https://www.theosthinktank.co.uk/comment/2020/09/23/the-social-dilemma-and-the-human-question

[11] Jacob Leon Kröger, Philip Raschke, and Towhidur Rahman Bhuiyan, "Privacy Implications of Accelerometer Data: A Review of Possible Inferences", https://dl.acm.org/doi/pdf/10.1145/3309074.3309076. See also: https://www.mayoclinicproceedings.org/article/S0025-6196(19)30063-1/fulltext

[12] Wu Youyou et al., "Computer-based personality judgments are more accurate than those made by humans", *Proceedings of the National Academy of Sciences* 112.4 (2015), pp. 1036-1040.

[13] Rachel Metz, "The smartphone app that can tell you're depressed before you know it", *MIT Technology Review*, 15 October 2018, https://www.technologyreview.com/2018/10/15/66443/the-smartphone-app-that-can-tell-youre-depressed-before-you-know-it-yourself/

[14] "Digital records could expose intimate details and personality traits of millions", Cambridge Psychometrics Centre, 11 March 2013, https://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions

[15] See Michal Kosinski et al., "Private traits and attributes are predictable from digital records of human behavior", *Proceedings of the National Academy of Sciences* 110.15 (2013), pp. 5802-5805. Michal Kosinski et al., "Mining big data to extract patterns and predict real-life outcomes", *Psychological Methods* 21.4 (2016), pp. 493-506.

[16] John Danaher, "Freedom in an Age of Algocracy" in Shannon Vallor (ed), *The Oxford Handbook of Philosophy of Technology* (Oxford: Oxford University Press, 2022), p. 257. Algocracy is defined as "a governance system in which computer coded algorithms structure, constrain, incentivize, nudge, manipulate or encourage different types of human behavior."

[17] Robert Elliott Smith, *Rage Inside the Machine*, Kindle version, 2%.

[18] The legal framework for social media platforms consists of a particular set of policy choices rooted in a neoliberal capitalist model. See Rachel Bovard, "Rule Social Media, or Be Ruled by It", *The New Atlantis*, Winter 2022, https://www.thenewatlantis.com/publications/rule-social-media-or-be-ruled-by-it

[19] Andy Crouch, *The Life We're Looking For* (New York, NY: Convergent, 2022), p. 29.

[20] Alan Jacobs, "Between Chaos and the Man", *Harper's Magazine*, December 2022.

2
Case study – social media

Having described the logic and workings of digital surveillance and the predictive power of machine learning systems in Chapter 1, this chapter offers a closer look at the way these play out with regards to social media. Social and political consequences of social media platforms that operate on a surveillance model are discussed in the second and third part of the chapter.

> “
>
> Social media platforms depend on grabbing and manipulating people’s attention.

When it comes to social media platforms, the surveillance system described in the previous chapter depends fundamentally on grabbing and manipulating people’s attention.[1] Social platforms are designed with a clear, overriding objective: to maximise “engagement” – any action a user might undertake on a platform: posting, scrolling, swiping, sharing, liking, and so on. Of course, engagement also means just time spent on the platforms, which translates into exposure to targeted ads, the main means by which Meta and Google generate revenue.

Social consequences of social media

This core feature of the surveillance and attention-capture model lies at the root of the extensive harms which are by now commonly associated with social media. Dealt with in more detail below, they include addiction and poor mental health, the proliferation of disinformation and extremist content.[2]

Many of the techniques used in the design of digital platforms have been developed at the Persuasive Technology Lab, a research centre within Stanford University, founded by B J Fogg, author of several volumes on persuasive digital technologies.[3] Tellingly, the name of the lab was changed to Behavior Design Lab, an acknowledgement that the research is geared towards behaviour modification.

Persuasive technology, as Tristan Harris argues, is intentionally designed to take advantage of human weaknesses and susceptibilities. Harris explains how design features like "pull to refresh", found on most social media platforms, are borrowed from the gambling industry. Pull to refresh, like slot machines, offers intermittent and variable "rewards which create little addictions".[4] Similarly, the "infinite scroll" feature, whereby users are shown a seemingly infinite string of content, lacks "stopping cues".[5] This heavily conditions users to stay on the platform. While it is important not to deny human agency and the ability, however conditioned and eroded, to exercise self-control, the fight against technology optimised for compulsive behaviour and addiction is emphatically not a fair one. Harris explains: "You can try having self-control, but there are a thousand engineers on the other side of the screen working against you."[6] Not only are platforms designed to be as addictive as possible, but the algorithms that power them are also fine-tuned, in real time, to push the content that maximises engagement – the perfect YouTube video to auto-play or news feed post to show next. For example, a *Wall Street Journal* investigation found that TikTok only needs one important piece of information to figure out what you want: the amount of

time you linger over a piece of content. Every second you hesitate or rewatch, the app is tracking you.[7]

These are just a few examples of how current social media design leads to compulsive and addictive behaviour, with harmful effects for personal and societal wellbeing. Other design choices and features, such as the "Follow" or "Like" button, have been designed to play on and exploit the inborn human desire for social approval, validation, and attention from others.[8]

This has arguably fuelled anxiety-inducing social comparison and the rise of "influencer" culture, particularly through Instagram and TikTok, but also acute self-consciousness and a mental health crisis for teenagers, particularly for teenage girls.[9]

To this end, researchers Jean Twenge and Jonathan Haidt have been collecting the academic literature on teen mental health and social media use.[10] Their work points to a marked increase in teen depression from 2010 onwards, particularly among girls, hospital admissions related to self-harm (for girls only) and suicide, since the advent of social networking sites, and particularly visually oriented platforms such as Instagram,[11] Snapchat and other similar "performative social media" platforms. Facebook's own research, leaked by the whistleblower Frances Haugen, has a similar finding: "Teens blame Instagram for increases in the rate of anxiety and depression... This reaction was unprompted and consistent across all groups."

The researchers also noted that “social comparison is worse on Instagram than on rival apps.”[12]

“

The problems associated with social platforms emerge as logical consequences of the “extractive business model of advertising ”.

Harris and other critics insist on the fact that the problems associated with social platforms are rooted in and emerge as logical consequences of the “extractive business model of advertising”. This is creating a growing asymmetry between the power of technology, as deployed by Big Tech, particularly social platforms, and the limits of human nature. This leads Harris to the conclusion that the relationship between any one individual user and technology companies is not a contractual one, between equals, but highly asymmetrical because of the disparity in information and the power derived from it that companies possess. Similarly, legal scholar Frank Pasquale refers to this situation as a “one-way mirror”, where “important corporate actors have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how they use this knowledge to influence the important decisions that we—and they—make.”[13] Due to the extensive knowledge advertisers have about the individual characteristics, preferences, and biases of consumers, targeting strategies can be perfectly calibrated. They can draw on both internal factors (e.g. low self-esteem) or external ones (e.g. being in financial difficulty) for maximum effectiveness when applying pressure.[14] Next to exploiting vulnerabilities, targeting can potentially result in other situations of unfairness. The case of Facebook selling advertisers the profiles of Australian teenagers that feel insecure goes to show there are vulnerable groups in society whose very vulnerability and weakness is exploited for commercial gain.[15]

Subverting democracy

Are platform companies, including but not exclusively social media ones, compatible with democracy?[16] In the early 2010s, especially around the time of the "Arab Spring", many would have answered in a resounding yes. Social media was seen as conducive to democracy, as ordinary citizens organised protests, expressed dissent towards authoritarian regimes, and managed to end them in some cases, if only temporarily. Subsequent years, however, have proven that social media platforms can be used just as well to squash democratic initiatives and undermine the democratic process itself, through tactics such as voter suppression and targeted political advertising. For example, in the 2016 US election, Russia created thousands of fake social media accounts to spread disinformation and other fabrications to support the candidacy of Donald Trump over Hillary Clinton.[17] More recent examples that have risen to public attention are the widespread proliferation of conspiracy theories and misinformation about COVID-19 and vaccines.

Probably the most consequential events that highlighted the precarious relationship between social media and democracy were those surrounding the end of the Trump presidency: the baseless and repeatedly shared claims that the US presidential election had been stolen, which led ultimately to the assault on the Capitol building in Washington on 6 January 2021 following President Trump's thinly veiled call to violent insurrection and attack on the US government. The events are currently under full investigation. In response to Trump's call, social media platforms banned President Trump.

There is clear evidence that those plotting the attack on the Capitol organised themselves using social media platforms.[18] Furthermore, despite Facebook's official statement from 1 July 2020 that the company "does not benefit from hate"[19], in the run up and aftermath of the attack on the Capitol, Facebook was seen to be "showing military gear ads next to insurrection posts".[20]

Facebook has admittedly made some efforts at mitigating the spread of extreme content, such as pornography, suicides, or live shooting spree videos,[21] with the use of algorithmic and human-generated content moderation. Yet as whistleblower Frances Haugen and other critics have shown, these are fundamentally reactive measures and therefore limited in what they can achieve, not to mention the traumatic effects that viewing violent and disturbing content, such as rapes and suicides in some cases, has on human moderators.[22] Furthermore, content moderation and censorship end up having a damaging effect on society and the democratic process as corporates and their impersonal algorithmic systems arbitrarily adjudicate opinions and values. This is not to suggest that content moderation should be stopped altogether, but that design-based solutions are arguably more sustainable and democracy-friendly. As Frances Haugen and the Center for Humane Technology have argued, introducing more friction in the sharing of content on social platforms, by removing the share button after two levels of sharing, or limiting the ability of users to reply to or interact with users they don't follow[23], for example, can more effectively prevent the sharing of harmful content and protect free speech at the same time.[24]

In the meantime, the erosion of democracy and social cohesion play out at several levels and in different yet connected ways.

First, social media is significantly behind the rise of misinformation.[25] An extensive study conducted by researchers at MIT and published in *Science* magazine in 2018 found that disinformation and misinformation spreads faster, farther, deeper, and more broadly than factually true information and stories:

> *False news stories are 70 percent more likely to be retweeted than true stories are. It also takes true stories about six times as long to reach 1,500 people as it does for false stories to reach the same number of people. When it comes to Twitter's "cascades," or unbroken retweet chains, falsehoods reach a cascade depth of 10 about 20 times faster than facts. And falsehoods are retweeted by unique users more broadly than true statements at every depth of cascade.*[26]

Explaining their methods, the researchers indicated that the study excluded "bots" designed to spread false information from the data sets. Asked what accounts for the phenomenon, they pointed to human psychology: the preference for novelty combined with social approval – something social platforms like Facebook and Twitter facilitate and exploit: "False news is more novel, and people are more likely to share novel information", to be shown in the know on social networks, said Sinan Aral, a Professor of Management at MIT.[27]

Connected to this, social media platforms have driven a proliferation of conspiracy theories with real life and troubling effects: from the Pizzagate conspiracy theory[28] to QAnon and the 6 January attack on the Capitol building in the USA. A *Scientific American* study from 2018 has shown how the wide spread of misinformation and disinformation on social media is enabled by a combination of cognitive, social, and algorithmic biases. Cognitive and social biases are rooted in human psychology. The study shows how in situations of "information overload", the brain applies several tricks to sort through information, including selecting for information that conforms to pre-existing beliefs and values.[29] Timothy Snyder writes: "Social media is no substitute: It supercharges the mental habits by which we seek emotional stimulation and comfort, which means losing the distinction between what feels true and what actually is true."[30]

So too, it is by now widely known that social media as currently designed, leads to the creation and reinforcement of "echo chambers" also known as "filter bubbles".[31] Perhaps an even better term is "micro-cultures",[32] which signals that these communities have their particular norms, values, and basic orientation to the world. They erode the possibility of agreeing on a common set of facts about the world. This, in turn, undermines the possibility of people who hold to different beliefs and values to converse and debate about the good and the shape the world should take, a foundational practice in well-functioning democracies. What emerges is a sort of cognitive loneliness as individuals see content that is curated to their tastes, preferences, and biases.[33]

By algorithmically curating increasingly extreme content to generate engagement, social media amplifies polarisation. Social media alone should not be blamed for the polarisation of public opinion. The collapse of the centre of politics and the tendency to gravitate to the edges of political opinion predate social media. But there is now clear evidence that social media, as part of the wider surveillance economy predicated on behavioural/predictive advertising, has deepened polarisation. Facebook's own internal studies have driven home this point time and again. For example, in 2017, an internal task force at Facebook found a clear correlation between the company's overriding objective of maximising user engagement and higher levels of political polarisation. In 2018, the task force proposed a series of fixes, including tweaking the algorithms to suggest a wider set of groups for people to join, but because the measures were acknowledged as "antigrowth", they were rejected by the company and the task force was dissolved.[34]

Increase in polarisation is something felt in everyday conversation as much as in the way traditional media outlets, in print, television, and radio, have been "disciplined" by social media. This can be seen in the way traditional media felt compelled to turn the rhetorical notch up in clickbait stories and headlines.

> **There is growing evidence that social media is corrosive to trust in governments, traditional news media, institutions, and people in general, amplifying polarisation and populism.**

More generally, there is growing evidence that social media is corrosive to trust in governments, traditional news media, institutions, and people in general, amplifying polarisation and populism. A working paper led by social scientists Philipp Lorenz-Spreen and Lisa Oswald concludes that there are clear causal links between digital media use and a decline in political trust, rise of populism, and growing polarisation, all of which do not bode well for the future of democracy.[35]

One of the most interesting revelations to come out of Facebook whistleblower Frances Haugen’s testimony was how European political parties felt compelled to run negative campaigns due to Facebook’s algorithm. Haugen said European political parties contacted Facebook to say that the newsfeed algorithm change, introduced to prioritise content that increases user engagement, was forcing political parties to take more extreme political positions in order to win users’ attention. Describing politicians’ concerns, she said: “You are forcing us to take positions that we don’t like, that we know are bad for society. We know if we don’t take those positions, we won’t win in the marketplace of social media.”[36]

In conclusion, giant social media companies exert a negative, disciplining effect on democracy and social cohesion through their monopoly power, on the economic front, and their power to shape beliefs, values, and behaviour, on the social and political front. As Francis Fukuyama, Barak Richman, and Ashish Goel of Stanford University note in a Foreign Affairs paper from 2019, “these behemoths now dominate the dissemination of information and the coordination of political mobilization. That poses unique threats to a well-functioning democracy.”[37]

The next chapter examines two further areas where the surveillance system plays out: facial recognition technology and predictive policing. Both distill and bring to light many of its troubling dynamics, including the harms and injustices they perpetuate, and therefore make for illuminating case studies.[38]

[1] See, among others, Tim Wu, *The Attention Merchants: How Our Time and Attention Are Gathered and Sold* (London: Atlantic Books, 2017) and Brett Frischmann and Evan Selinger, *Re-Engineering Humanity* (Cambridge, UK: Cambridge University Press, 2018).

[2] Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar", *Meta*, 5 November 2018, https://about.fb.com/news/2018/11/myanmar-hria/

[3] Fogg's books include *Persuasive Technologies* (2003) and *Mobile Persuasion* (2008).

[4] Tristan Harris testimony in the US Senate, p. 1, https://www.commerce.senate.gov/services/files/96E3A739-DC8D-45F1-87D7-EC70A368371D

[5] At the time of writing, only TikTok has introduced screen time controls. Twitter, Instagram, Facebook still operate with an "infinite scroll".

[6] Ibid. 4.

[7] "Investigation: How TikTok's Algorithm Figures Out Your Deepest Desires", *Wall Street Journal*, 21 July 2021, https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796

[8] Ibid.

[9] Jonathan Haidt, "The Dangerous Experiment on Teen Girls", *The Atlantic*, 21 November 2021, https://www.theatlantic.com/ideas/archive/2021/11/facebooks-dangerous-experiment-teen-girls/620767/

[10] Jonathan Haidt and Jean Twenge (ongoing), "Adolescent mood disorders since 2010: A collaborative review", unpublished manuscript, New York University, https://docs.google.com/document/d/1diMvsMeRphUH7E6D1d_J7R6WbDdgnzFHDHPx9HXzR5o/edit

[11] Jonathan Haidt, "The Dangerous Experiment on Teen Girls". See also: Jonathan Haidt, "Why the Past 10 Years of American Life Have Been Uniquely Stupid", *The Atlantic*, 11 April 2022, https://www.theatlantic.com/magazine/archive/2022/05/social-media-democracy-trust-babel/629369/

[12] "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show", *Wall Street Journal*, 14 September 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[13] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2016), p. 9.

[14] Karen Yeung, "Five fears about mass predictive personalisation in an age of surveillance capitalism", *International Data Privacy Law*, vol. 8, no. 3 (2018), pp. 258-269, http://pure-oai.bham.ac.uk/ws/files/54479954/

Yeung_Five_Fears_About_Mass_Personalisation_Final_for_Submission_2018.pdf.

15 Sam Machkovech, “Report: Facebook helped advertisers target teens who feel ‘worthless’”, *Ars Technica*, 1 May 2017, https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/.

16 See Paul Nemitz, “Constitutional technology and democracy in the age of artificial intelligence”, *Philosophical Transactions of the Royal Society A*, vol. 376, issue 2133 (2018), https://doi.org/10.1098/rsta.2018.0089.

17 “Russian active measures campaigns and interference in the 2016 US election. Volume 2: Russia’s use of social media with additional views”, Select Committee on Intelligence, United States Senate: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

18 Jason Thacker, “Jan. 6 was fueled by misinformation. More content moderation won’t fix it”, *The Week*, 6 January 2022, https://theweek.com/facebook/1008627/jan-6-was-fueled-by-misinformation-more-content-moderation-wont-fix-it?utm_source=links&utm_medium=website&utm_campaign=twitter

19 Nick Clegg, “Facebook Does Not Benefit from Hate”, *Meta*, 1 July 2020, https://about.fb.com/news/2020/07/facebook-does-not-benefit-from-hate/

20 Ryan Mac and Craig Silverman, “Facebook Has Been Showing Military Gear Ads Next To Insurrection Posts”, *BuzzFeed News*, 14 January 2021, https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot

21 Colleen Murrell, “The Christchurch shooting was streamed live, but think twice about watching it”, *ABC* News, 15 March 2019, https://www.abc.net.au/news/2019-03-15/christchurch-shooting-live-stream-think-twice-about-watching-it/10907258

22 “Facebook to pay $52m to content moderators over PTSD”, *BBC News*, 13 May 2020, https://www.bbc.co.uk/news/technology-52642633

23 David French, “The ‘Twitter Files’ Show It’s Time to Reimagine Free Speech Online”, *Persuasion newsletter*, https://open.substack.com/pub/persuasion1/p/the-twitter-files-show-its-time-to?r=5fih2&utm_campaign=post&utm_medium=email

24 “Make Facebook #OneClickSafer”, *Center for Humane Technology*, https://www.humanetech.com/oneclicksafer. See their #OneClickSafer campaign.

25 Anne Applebaum and Peter Pomerantsev, “How to Put Out Democracy’s Dumpster Fire”, *The Atlantic*, April 2021, https://www.theatlantic.com/magazine/archive/2021/04/the-internet-doesnt-have-to-be-awful/618079/

26 Peter Dizikes, “Study: On Twitter, false news travels faster than true stories”, *MIT News*, 8 March 2018, https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308

27 Ibid.

28 “Pizzagate conspiracy theory”, *Wikipedia*, https://en.wikipedia.org/wiki/Pizzagate_conspiracy_theory

29 Giovanni Luca Ciampaglia and Filippo Menczer, “Biases Make People Vulnerable to Misinformation Spread by Social Media”, *Scientific American*, 21 June 2018, https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/

30 Timothy Snyder, “The American Abyss: A historian of fascism and political atrocity on Trump, the mob and what comes next”, *The New York Times Magazine*, 9 January 2021, https://www.nytimes.com/2021/01/09/magazine/trump-coup.html

31 Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You* (New York, NY: Penguin, 2011).

32 L M Sacasas, “The Insurrection Will Be Live Streamed: Notes Toward a Theory of Digitization”, *The Convivial Society*, 15 January 2021, https://theconvivialsociety.substack.com/p/the-insurrection-will-be-live-streamed. Sacasas argues that in our context of information superabundance, what he calls the Database precedes the Narrative. He explains: “It’s not just that there is widespread disagreement about how to interpret the meaning of an event. It is also that there is widespread disagreement about the basic facts of the event in question. It is one thing to argue the meaning of the moon landing for human affairs, it is another to incessantly debate whether the moon landing happened.” In light of this reading he puts forth the intriguing and indeed disarming proposition that “we are all conspiracy theorizers now”, explaining that “we are all in the position of holding beliefs, however sure we may be of them, that a sizable portion of the population considers not just mistaken but preposterous and paranoid.” To make matters worse, or at least more complex, it is far from clear this is a situation that obtains only because of social media as it functions today. His claim is stronger: this is an internet and information age predicament – our very informational environment.

33 Hannah Arendt chillingly warned that this is fertile ground for a form of “totalitarian domination in a non-totalitarian world”: “What prepares men for totalitarian domination in the non-totalitarian world is the fact that loneliness, once a borderline experience usually suffered in certain marginal social conditions like old age, has become an everyday experience.” See Hannah Arendt, *The Origins of Totalitarianism* (1951). See also: Samantha Rose Hill, “Where loneliness can lead”, *Aeon*, 16 October 2020, https://aeon.co/essays/for-hannah-arendt-totalitarianism-is-rooted-in-loneliness

[34] Karen Hao, "How Facebook got addicted to spreading misinformation", *MIT Technology Review*, 11 March 2021, https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/

[35] Philipp Lorenz-Spreen, Lisa Oswald, Stephan Lewandowsky, and Ralph Hertwig, "A Systematic Review of Worldwide Causal and Correlational Evidence on Digital Media and Democracy", *SocArXiv Papers*, 7 November 2022, https://osf.io/preprints/socarxiv/p3z9v/. See also: Jonathan Haidt, "Why the Past 10 Years of American Life Have Been Uniquely Stupid", https://www.theatlantic.com/magazine/archive/2022/05/social-media-democracy-trust-babel/629369/

[36] Dan Milmo, "Facebook 'tearing our societies apart': key excerpts from a whistleblower", *The* Guardian, 4 October 2021, https://www.theguardian.com/technology/2021/oct/04/facebook-tearing-our-societies-apart-key-excerpts-from-a-whistleblower-frances-haugen

[37] Francis Fukuyama, Barak Richman, and Ashish Goel, "How to Save Democracy From Technology: Ending Big Tech's Information Monopoly", *Foreign Affairs*, vol. 100.1 (Jan/Feb 2021), p. 98.

[38] See Kate Crawford, *Atlas of AI,* Chapter three: "Data", pp. 89-123.

3

Case study – facial recognition technology and predictive policing

Facial recognition

What is facial recognition technology and how does it work?

Privacy scholar Woodrow Hartzog and tech philosopher Evan Selinger consider facial recognition to be "the most uniquely dangerous surveillance mechanism ever invented… a menace disguised as a gift."[1] As an "all-out privacy-eviscerating machine", it is, they argue, a perfect tool of oppression and authoritarian control.

The first thing to note is that facial recognition systems exist on a spectrum. At one end, we find relatively simple systems that merely pick out faces, such as phone cameras that detect human faces in real time or digital albums which sort pictures according to the faces identified. Then there are systems that analyse faces without storing the data, as in the case of interactive billboards. Other systems simply provide facial verification, for example, in the case of iPhone's Face ID feature, which matches the user's face with a securely saved template – or, in the case of visually impaired persons, through audio and braille interfaces. This is called one-to-one identification. In these cases, biometric data (data about human physical and behavioural characteristics – e.g. fingerprints, voice, gait) is either not collected at all (in the case of mere face detection) or stored locally in a closed-circuit system (for example, in the face unlocking feature on newer models of iPhone).

These are quite different from facial recognition systems which most concern privacy and civil rights activists. What we might call “facial recognition proper” is facial recognition technology that practices “one-to-many” identification, thus allowing it (through the use of recognition algorithms) to identify individuals, often in real time, by scanning the data inputted from cameras against vast image databases with millions of faces (e.g. police databases of mugshots and driver licence images). The image banks themselves, it must be stressed, raise concerns on their own, given that often the biometric data have been scraped without consent from sources as diverse as social media profiles and video streaming sites, among other sources.

What is wrong with it?[2]

One of the most-discussed issues with facial recognition technology is the low-quality or even flawed data fed by law-enforcement agencies.[3] This makes misidentification more likely. Second, the proximate harms of facial recognition technology include a chilling effect on people expressing themselves in public, including in religious gatherings or when protesting. Self-censorship is a well-known effect on people who know they are being monitored.

There is growing evidence that facial recognition technologies have a disproportionately negative impact on people of colour and other minority and vulnerable populations.[4] False positives, false negatives, and other forms of misidentification can lead to innocent people being surveilled, sometimes quite aggressively and covertly, falsely charged, and even arrested for crimes of which they

> “
>
> **There is growing evidence that facial recognition technologies have a disproportionately negative impact on people of colour and other minority and vulnerable populations.**

were innocent. This is not simply a miscarriage of justice, but an attack on human dignity.

Employing facial recognition technology shifts the ideal from "presumed innocent" to "people who have not been found guilty of a crime yet" but who are nevertheless surveilled (see below the case study on predictive policing).[5]

The case of FindFace app, which deploys facial recognition software to match random photographs to people's social media pages, illustrates how facial recognition invited abusive uses such as harassment and even violence. This was the case of several Russian women who appear in pornographic material, whose identities were revealed by hackers using FindFace's facial recognition capabilities.[6]

At a more basic level, extensive use of facial recognition, which is arguably a growing trend, can lead to a denial of fundamental rights and opportunities, such as protection against "arbitrary government tracking of one's movements, habits, relationships, interests, and thoughts".[7]

Facial recognition also leads to a progressive elimination of practical obscurity – a key dimension of privacy that has to do with conditions that allow people to not be easily identified. One enjoys obscurity, for example, in large crowds, on busy streets, or in a crowded restaurant.[8]

All of the above add up to amplifying surveillance capitalism and the surveillance culture it engenders. For example, as part of a "flood the market" strategy, the facial recognition company Clearview.AI offered "free trials" to more than 7,000 individuals from over 1,800 public agencies in the US without any purchasing agreement or contract and, crucially, without any public oversight.[9]

In addition to the above, a deeper problem, as Selinger and Hartzog note, is that, once introduced, the surveillance material infrastructure of facial recognition technology is unlikely to be rolled back. This aids "surveillance creep" and applications whose impact cannot be realistically ascertained in advance.

Like other surveillance technologies, facial recognition promises an increase in security. While this may be true, it also simultaneously entrenches the power asymmetry it depends upon and articulates, and thus invites overreach and "mission creep".[10]

> **Facial recognition promises an increase in security but it simultaneously entrenches the power asymmetry it depends upon and articulates.**

There are grave and widely shared concerns in their own right around the use of sensitive data (i.e. human faces). The human face is inescapably wrapped up with one's identity and self-presentation in the world. Faces, as Hartzog explains, are "the conduits between our on- and offline lives, and they can be the thread that connects all of our real-name, anonymous, and pseudonymous activities."[11] They are also what enable social recognition, a key ingredient in functioning societies. Moreover, the face, as Jewish philosopher Emmanuel Levinas has memorably argued, can also be a site where ethical relationships and responsibility take shape.[12]

It is generally hard to hide or modify one's face and the data cannot be encrypted. Moreover, faces can be captured at a distance without the subject's awareness. While more information can be inferred from faces than any other biometric (i.e. facial characterisation), critics point out that inferences about a persons' sexual orientation or presumed propensity for criminal behaviour, for example, are often based on dubious science. This does not, however, prevent such inferences from being made and sold by data brokers to various stakeholders, including law enforcement, marketers, educators, and other groups.[13] The data can be stored easily and inexpensively as advances in storage capabilities continue to increase and reduce in price. Furthermore, as Hartzog notes, there is an abundance of data already available, in contrast to other forms of surveillance. Images of faces are constantly being recorded through CCTV cameras and body-cams worn by police.

What is (to be) done about it?

Civil rights and other advocacy bodies have been calling for the complete ban of facial recognition technology by the US government. In the UK, Big Brother Watch has been engaged in similar efforts. Various groups have been asking Amazon to stop selling its facial recognition technology, Rekognition, to law enforcement agencies.[14] A number of states and municipalities in the US have been deliberating and, in some cases, enacting bans on the technology.[15] The EU had been considering a five-year moratorium on the technology[16] but these plans have been scrapped at the time of writing.[17]

Many, like Woodrow Hartzog and Evan Selinger, are calling for a complete ban on it, seeing it as a technology that renders people fully transparent and vulnerable to unaccountable actors, comprehensively trackable, therefore compromised. They argue that "the future of human flourishing depends" on banning this technology before it becomes normalised and entrenched in our lives.[18]

Predictive policing

What is it? How does it work? What is to be done?

Another controversial application of AI at the intersection of surveillance and algorithmic decision-making is predictive policing. Predictive policing[19] refers to a set of technologies used by law enforcement agencies and police departments to forecast criminal activity and allocate police resources. These technologies feed on historical crime data (mainly location, type, and time of crime) to generate predictions of where future crimes are likely to occur (if they pertain to geographical areas), or which individuals are likely to commit crimes (if they are targeted at individuals).[20] Current research suggests predictive policing relies on inaccurate, skewed, or systematically biased "dirty data",[21] which illustrates the so-called "garbage in/garbage out" problem in data analytics. More significantly, predictive policing is itself an illustration of how technology

> **Predictive policing entrenches injustices and inequalities by targeting and over-policing areas made up predominantly of people of colour and the economically disadvantaged.**

is never neutral, but "productive" (formative) and morally loaded. This notion is exemplified below.

Predictive policing entrenches injustices and inequalities by targeting and over-policing areas made up predominantly of people of colour and the economically disadvantaged.[22] For example, in Amsterdam local authorities have compiled a list of 400 young people ordered according to their algorithmically determined likelihood of engaging in criminal activity. Many youth from deprived neighbourhoods ended up on the list without having committed any criminal offences.[23] The evidence is that data-driven policing is rarely used to address so-called "white collar crimes", such as wage theft and property crimes. It is almost invariably deployed to combat crimes associated with groups that have faced historic discrimination and injustice:

> *The algorithmic crystal ball that promises to predict and forestall future crimes works from a fixed notion of what a criminal is, where crimes occur, and how they are prosecuted (if at all). Those parameters depend entirely on the power structure empowered to formulate them—and very often the explicit goal of those structures is to maintain existing racial and wealth hierarchies.*[24]

Predictive policing entails a future that is made entirely from the past – a past recycled as self-fulfilling predictions.

At a more philosophical level, predictive policing entails a future that is made entirely from the past – a past recycled as self-fulfilling predictions:

> *Because of police data from the past, McDaniel's neighborhood, and therefore the people in it, were labelled as violent... the program then said that the future would be the same—that is, that there*

> *would not be a future, but merely reiterations of the past, more or less identical with it. This is not merely a self-fulfilling prophecy, though it certainly is that: It is a system designed to bring the past into the future, and thereby prevent the world from changing.*[25]

It assumes that what is contingent in history will be an inevitability in the future. This is a form of fatalism where the open-endedness of the future is replaced with a closed, pseudo-future which functions in a closed loop with the past. Such a scenario, where one's past failures hang over oneself indefinitely, is dystopian and amounts to a violation of human dignity. Indeed, the dignity of human beings in their irreducible particularity is what is ultimately at stake when we consider the surveillance system.

As the next chapter will seek to show, a re-imagined notion of privacy, placed on a wider, anthropological foundation, will help clarify the deeper ethical concerns that arise in connection to the surveillance system and provide a strong basis for addressing them, including the injustices associated with the use of facial recognition technology and data-driven policing.

[1] Woodrow Hartzog, “Facial Recognition Is the Perfect Tool for Oppression”, *Medium*, 2 August 2018, https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66. See also Joy Buolamwini, Vicente Ordóñez, Jamie Morgenstern, and Erik Learned-Miller, “Facial Recognition Technologies: A Primer”, 29 May 2020, https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

[2] Two reports, among others, thoroughly detail many of the problems associated with facial recognition: a paper written by Jennifer Lynch, senior staff attorney at the Electronic Frontier Foundation and The Perpetual Line-Up study from Georgetown’s Center on Privacy and Technology, co-authored by Clare Garvie, Alvaro Bedoya, and Jonathan Frankle. See: https://www.eff.org/files/2020/04/20/face-off-report-2020_1.pdf; https://www.perpetuallineup.org/

[3] See Clare Garvie, “Garbage In, Garbage Out: Face Recognition on Flawed Data”, *The Center on Privacy & Technology at Georgetown Law*, 16 May 2019, https://www.flawedfacedata.com

[4] “The Color of Surveillance”, *Georgetown Law*, https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017/; https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/

[5] Anne-Marie Slaughter and Stephanie Hare, “Our Bodies or Ourselves”, *Project Syndicate*, 23 July 2018, https://www.project-syndicate.org/commentary/dangers-of-biometric-data-by-anne-marie-slaughter-and-stephanie-hare-2018-07

[6] Kevin Rothrock, “Facial recognition service becomes a weapon against Russian porn actresses”, *Ars Technica*, 26 April 2016, https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/

[7] Kimberly L Wehle, “Anonymity, Faceprints, and the Constitution”, *George Mason Law Review,* vol. 21, no. 2 (Winter 2014), pp. 409-466, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394838

[8] Evan Selinger and Woodrow Hartzog, “Obscurity and Privacy”, *Routledge Companion to Philosophy of Technology* (Joseph Pitt and Ashley Shew, eds, 2014 Forthcoming). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439866

[9] Tate Ryan-Mosley, “How US police use counterterrorism money to buy spy tech”, *MIT Technology Review*, 7 December 2022, https://www.technologyreview.com/2022/12/07/1064354/police-counterterrorism-money-buy-spy-tech-surveillance-fema/?truid=&utm_source=the_algorithm&utm_medium=email&utm_campaign=the_algorithm.unpaid.engagement&utm_content=12-12-2022&mc_cid=59d8f27a92&mc_eid=b53e890970. See also:

"Surveillance Nation", *BuzzFeed News*, 10 April 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition

10 The Internal Revenue System (IRS) in the US, for example, planned to require taxpayers to undergo facial recognition scans to access their tax accounts. This was revoked following successful campaigning led by, among others, Joy Buolamwini: "The IRS Should Stop Using Facial Recognition", *The Atlantic*, 27 January 2022, https://www.theatlantic.com/ideas/archive/2022/01/irs-should-stop-using-facial-recognition/621386/?mc_cid=4788f60c95&mc_eid=b53e890970

11 Woodrow Hartzog, "Facial Recognition Is the Perfect Tool for Oppression", *Medium*, 2 August 2018, https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

12 See also Roger Scruton, *The Face of God* (London, Continuum: 2014).

13 Evan Selinger and Brenda Leong, "The Ethics of Facial Recognition Technology", 7 January 2021. Forthcoming in *The Oxford Handbook of Digital Ethics* (Carissa Véliz, ed). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762185

14 David Jeans, "Amazon Facing Calls From Civil Rights Groups To Permanently Ban Police Use Of Facial Recognition As Deadline Approaches", *Forbes*, 11 May 2021, https://www.forbes.com/sites/davidjeans/2021/05/11/amazon-facial-rekognition-ban-civil-rights-groups/?sh=38c93e07325e

15 "The Fight Against Government Face Surveillance: 2019 Year in Review", *Electronic Frontier Foundation*, 31 December 2019, https://www.eff.org/deeplinks/2019/12/year-fight-against-government-face-surveillance. See also: "California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams", *ACLU of Northern California*, 8 October 2019, https://www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams

16 Janosch Delcker and Bjarke Smith-Meyer, "EU considers temporary ban on facial recognition in public spaces", Politico, 16 January 2020, https://www.politico.eu/article/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces/

17 Foo Yun Chee, "EU drops idea of facial recognition ban in public areas: paper", *Reuters*, 29 January 2020, https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q

18 Woodrow Hartzog, "Facial Recognition Is the Perfect Tool for Oppression", https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

19 This is also known as "data-driven policing", terms that are meant to sound benign and ethically unproblematic.

[20] Andrew Guthrie Ferguson, "Surveillance and the Tyrant Test", *Georgetown Law Journal*, vol. 110, no. 2 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4016828

[21] Rashida Richardson, Jason M Schultz, and Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice", *New York University Law Review*, vol. 94:192, https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf

[22] See Kate Crawford, Meredith Whittaker et al., "AI Now 2019 Report", *AI Now Institute,* December 2019, https://ainowinstitute.org/AI_Now_2019_Report.html

[23] Mark Visser, "Young people who have done nothing will also be added to the Amsterdam Top 400 risk list", *Trouw*, 14 November 2022, https://www.trouw.nl/binnenland/ook-jongeren-die-niets-hebben-uitgehaald-komen-op-amsterdamse-risicolijst-top-400~b4d1680d/?mc_cid=e6b80ac47a&mc_eid=b53e890970

[24] Chris Gilliard, "Crime Prediction Keeps Society Stuck in the Past", *Wired*, 2 January 2022, https://www.wired.com/story/crime-prediction-racist-history/

[25] Ibid.

4
Re-imagining privacy

The privacy landscape

Although privacy is by no means the only lens to take, many of the ramifications of the surveillance system described in the previous sections of this essay are analysed through the lens of privacy. Indeed, privacy is a growing concern in our societies increasingly dominated by AI and digital technology. With its roots in the beginnings of European print culture and liberal democracy, privacy has come to be enshrined in law as a fundamental human right in the 1948 Universal Declaration of Human Rights (Preamble and Article 1), and the EU Charter of Fundamental Rights.[1]

More recently, privacy is at the heart of the EU's groundbreaking General Data Protection Regulation (GDPR). It is widely considered one of the key values threatened by surveillance capitalism and, as I sought to describe in Chapter 1, the widespread data harvesting and analytical operations on which it relies.[2]

> “
>
> **Privacy has come to act as a point of convergence between tech critics, regulators, and other stakeholders within civil society concerned with the data economy.**

The term privacy itself does a fair bit of heavy lifting and has come to act as a point of convergence between tech critics, regulators, and other stakeholders within civil society concerned with the data economy.[3] In response to the “techlash”, tech companies like Apple and Uber have ramped up their efforts to enhance privacy for their users, with Apple being particularly privacy conscious among tech companies.[4]

There is, moreover, a growing number of publications that deal with privacy. They both account for privacy's ongoing erosion and suggest various measures to protect it.[5] These range from measures individuals can take, like changing default settings on personal devices or websites' privacy settings, to systemic action in the form of government regulation, stockholder engagement, as well as innovations and technologies that take a "privacy by design" approach.[6]

Such is the landscape of digital privacy today. But according to legal scholar Daniel Solove, privacy is a "concept in disarray".[7] While regularly invoked, its precise meaning remains elusive. As noted in *The Rise of Privacy Tech* white paper on defining the privacy tech landscape, privacy can be understood in various valid ways. Below is a taxonomy of four of the most common:[8]

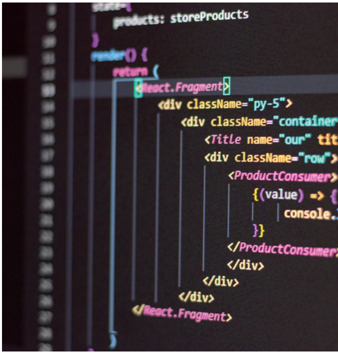
- As *control* or *power* over personal data flows; the ability to determine what information about oneself is being collected and processed, by whom, and on what terms.[9]
- As *obscurity*. As Woodrow Hartzog and Evan Selinger note, obscurity "is the idea that information is safe—at least to some degree—when it is hard to obtain or understand."[10] Obscurity therefore has to do with the accessibility and interpretation of information. Hartzog and Selinger explain: "The easier it is to find information, the less obscure it is, and the harder it is to locate information, the more obscure it is."[11]
- As *trust* – privacy is a social good that has to do with disclosures within relationships of trust between

people and between people and institutions.[12] In the relationships between an individual and an institution, this trust is expressed and nurtured through (1) honesty in data practices; (2) discretion in data usage; (3) protection of data against hostile outsiders; (4) a commitment to protect the persons whose data is handled.[13]

- As *conceptual integrity* – privacy is about what is appropriate for different groups to know about us given the nature of the information and the context in which it is shared. In others words, privacy is determined in context and is a function of variables such as: the nature of the situation or context; the nature of the information in relation to that context; on what terms the information is shared; the roles of agents receiving information.[14]

Digital privacy is clearly a bundled concept; a container for a diverse and interrelated set of concerns regarding harms and violations which arise at the nexus of data, machine learning algorithms, and the wider surveillance architecture. As privacy scholar Woodrow Hartzog shows, of the different ways privacy is understood today, control or power over one's data is the foundational aspect of privacy.[15]

One reason for this is pragmatic: most of the data generated by individuals – so data about them – is held unaccountably in the hands of, and used at the discretion of, any number of businesses and public institutions. The asymmetry between the individual "data subject" and the organisations who wield the data is stark, both in terms of the knowledge that the latter can derive about the former (as explained earlier in this essay) and the power, to influence and control, that accrues to such knowledge. So wresting back control over one's data, when so much has been eroded, is supposed to be a means of asserting personal agency in the face of powerful and impersonal corporate and government actors. But this framing of privacy as control over one's data flows is problematic on both practical and moral- anthropological grounds. From a practical point of view, it wrongly assumes that all the data we release or reveal are the result of deliberate acts.[16] This is often not the case. Chapter 1 has shown how Meta, for example, harvests (meta) data that most people wouldn't recognise as data in the first place: what we hover over or how long we hover for, how many tabs we have open, what operating system we use etc. If privacy is framed in terms of control, we bear the responsibility for these disclosures. Furthermore, this view does not reckon with the possibility that certain data revelations can be manipulated. As legal scholar Ari Ezra Waldman argues, "positive emotional feelings about a website, inspired by website design, the type of information requested, and the presence of a privacy policy, correlate with a higher willingness to disclose."[17] From a moral-anthropological point of view, this conception of privacy as individual control over data undermines our agency by placing impossible demands on it even as it tries to safeguard it. It overwhelms agency as it tries to uphold it. With this observation, we are firmly on a terrain where anthropological and wider moral assumptions – about the nature of the human, of freedom and flourishing – are not far under the surface. Indeed, the dominant understanding of privacy as control over personal information stems from the dominant, modern anthropology which sees human beings primarily as self-determining, morally

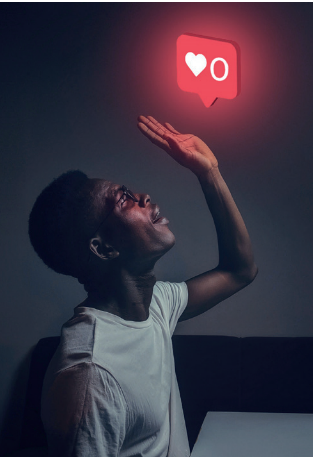


```
    state={
      products: storeProducts
    }
    render() {
      return (
        <React.Fragment>
          <div className="py-5">
            <div className="container
              <Title name="our" tit
              <div className="row">
                <ProductConsumer>
                  {(value) => {
                    console.
                  }}
                </ProductConsumer
              </div>
            </div>
          </div>
        </React.Fragment>
```

autonomous individuals. This can be seen in the way privacy is generally cast in individualistic terms, as an individual right, even as its social dimension and relevance are sometimes also acknowledged.[18]

In stronger articulations, privacy arises from a commitment to autonomy and self-determination. Zuboff, for example, represents a wide constituency in grafting privacy onto “moral autonomy” and “individual sovereignty”, and seeing the latter as “civilization’s necessary and final bulwark”,[19] uniquely threatened by surveillance capitalism.

Autonomy and self-determination are admittedly complex, multi-layered notions, which are often conflated or used in imprecise ways. Sometimes they are used to refer simply to human agency, which I define as the capacity to think, feel, and act without unwanted interference or coercion. Other times they stand for an individual’s presumed freedom to choose their own moral values. In the way she deploys the terms, Zuboff clearly leans towards the latter.[20]



Once again, we are deep in anthropological territory here – and so, beneath a vast array of the topical, technological, technical issues explored above, affecting our daily lives in ways stretching from the mundane to the sinister, we find the more fundamental question of what it means to be human. We must therefore step back and ask afresh the following questions: What does it mean to flourish as a human being in the digital age? What are we truly concerned about when we decry the erosion or loss of privacy? What values or social goods are we seeking to foster and protect? And why?

Asking such questions allows us to sidestep the ambiguity surrounding the concept of privacy and focus, as Solove himself advises, on the specific problems, harms, and violations we are concerned about as they emerge concretely. It also enables a more fruitful discussion, where all anthropological cards are, so to speak, on the table. As with every other matter, there is no view from nowhere.[21] Every ethics is underpinned by an anthropology, and every anthropology derives from a broader worldview or metaphysical framework, whether philosophical or religious. In the discussion that follows, I draw explicitly on Christian theological anthropology but gladly anticipate crossover with other religious and indeed non-religious anthropologies, which readers are welcome to identify.

Privacy and dignity – a theological perspective

Privacy is often raised in connection with human dignity. Privacy International, for example, defines privacy as "a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built."[22] Through this lens, privacy violations are seen as an assault on human dignity. This is right, but without specifying the meaning of dignity, the risk is that we explain one elusive concept (privacy) with another (dignity). Oxford academic and philosopher of information Luciano Floridi's challenge remains: "Unless one explains convincingly what human dignity may mean in the twenty-first century, it remains obscure and questionable exactly which interpretation of human dignity may provide the foundation for privacy (as well as all other human rights)."[23]

A detailed discussion of the different conceptions of dignity is beyond the scope of this essay. But it is worth mentioning one that prevails today: dignity as autonomy.

John Tasioulas, the director of the Oxford Institute for Ethics in AI and Professor of Ethics and Philosophy of Law at Oxford University, reflected in an interview that his "deepest fear is that AI will be corrosive of human dignity" but went on to identify dignity with the ability "to engage in rational self-determination".[24] This is a common but ultimately mistaken move when we take into consideration the most vulnerable members in our society: young children; the severely mentally disabled; or persons in minimally conscious states and deep comas, whose ability to engage in rational self-determination is either limited or altogether absent, and yet who remain deserving of the same dignity as everyone else. Surely, a more capacious and inclusive notion of dignity is needed.

> "
>
> **Dignity consists in being precisely the creatures human beings are: relational, agential and embodied.**

A theological perspective is relevant here. Christian thought roots human dignity not in any particular capacity or feature of being human, but transcendentally, through their identity in relation to God. All human beings have intrinsic and inalienable dignity in virtue of being created by God, bearing the "image of God", and being essentially related to God (whether they acknowledge it or not). Regardless of physical or mental ability, social standing or economic power, all human beings have this intrinsic value and worth. If this is the transcendental basis of human dignity, it consists in being precisely the creatures human beings are: *relational*, *agential* (i.e. with agency or the potential for it according to our stage or condition), *embodied*, and therefore

with *natural limitations, fragilities,* and *susceptibilities*. I briefly discuss the implications of these, as they relate to the question of privacy and the wider ethical concerns surrounding the surveillance culture, below.

Human beings as relational creatures

As created by a Trinitarian God, that is, a God whose own being is relationship of three Persons, human beings are fundamentally and irreducibly relational creatures. Relationship, with God (as Creator), with fellow human beings and the non-human world (as "neighbours") is constitutive of human beings. We are irreducibly persons in relationship rather than atomised individuals. We flourish in relationships of trust, interdependence, and intimacy and are diminished by lack of relationship and isolation.

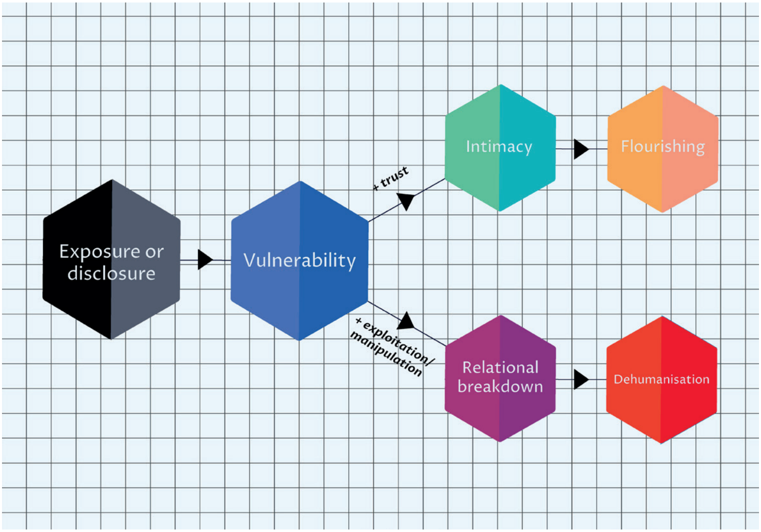
On this reading, at the deepest level of our being, we should not seek privacy as a means of control (either over one's own situation, or over others), but rather, insofar as it enables better, deeper, healthier relationships of trust and mutual care. To take an analogy, we do not seek the privacy of our own homes merely (practically) to shield ourselves from the world outside. Of course, such shielding is sometimes necessary, but it could just as easily be provided by a room with a locked door, and is certainly not an end in itself. Rather, if we are lucky enough to have a safe, dry dwelling place, we more profoundly *enjoy* the privacy of "home" as a space in (and from) which we can build family, host friends, and extend hospitality and generosity to others. In other words, privacy is an essential ingredient in flourishing as persons, but is valuable most of all as a precondition of intimacy (including but not reduced to sexual intimacy).[25]

How does this translate to the use and regulation of technology? Crucially, the main criteria for whether tech

companies are well regulated is not whether we can hide from them or not (though the ability to do so would be most welcome). Nor should the motivation to create spaces (online and offline) where we are empowered to build relationships for their own sake – rather than for self-interest or profit – be understood as just one of our motivations among many. Rather, it is foundational to our identity. There is a reason why Facebook advertises itself as a platform to "help you connect and share with the people in your life". This is what we really want. What is commodified by Meta and other social platforms is therefore not simply "my data" but my relationships.

Ironically, it is precisely this possibility of intimacy, and therefore of flourishing, which is threatened by the data harvesting practices detailed in this essay. With the expansion of the current surveillance system, our lives are rendered fully exposed or transparent to the gaze of impersonal Others – corporate, state, or otherwise. This exposure, in the absence of patiently cultivated and hard-earned trust, is experienced as total vulnerability, by some groups more than others, as the case studies above show.[26] This condition of vulnerability is both exploited and compounded by surveillance capitalist companies for profit or by state systems that perpetuate injustice, for example through the use of facial recognition and predictive policing.

> **What is commodified by Meta and other social platforms is therefore not simply "my data" but my relationships.**



A Christian defence of privacy begins not in the name of a fundamental, absolute right to self-determination of the individual but in the name of care for others, especially the most vulnerable in our midst.

This also means that privacy does not simply have to do with what others (e.g. advertisers or government agencies) know about me – an individual concern – but also with systems that my data feeds into, the consequences of which apply not simply to me but to my vulnerable neighbour. Such systemic implications are admittedly hard to pin down given the opaqueness of the way data circulates in the digital economy: how my data is aggregated with my

> “
>
> **A Christian defence of privacy begins not in the name of a fundamental, absolute right to self-determination of the individual but in the name of care for others, especially the most vulnerable in our midst.**

neighbour's data and with the data of billions of other individuals in the world; how it is fed into machine learning algorithms whose "decisions" are generally "black boxes", meaning that the process by which a decision is made is unknown and unknowable even for the creators of the said algorithm. Nonetheless, as we become more aware of the inner workings of these processes, the need to understand our use of technology as a form of "love of neighbour" becomes increasingly clear.

Human beings with agency and freedom

Another dimension of a Christian anthropology that is relevant for the purpose of re-imagining privacy is the notion of agency. As alluded above, agency can be defined simply as the capacity to think, feel, and act in the world, without coercion or unwanted interference.[27] There is clearly a developmental dimension to agency. We develop as persons through our activities in the world and in relation to others. Privacy is therefore a good because it understands the limits and boundaries of what makes a person (or indeed any creature) develop properly and thus flourish.[28]

But agency, like power, is unevenly distributed. Some people and groups have more agency than others. Indeed, one of the most ethically concerning issues about social platforms is the wide disparity of power and agency between them and individual "users". In short, social platforms have significant agency to influence and heavily condition a persons' perceptions, choices, and values. Similarly, institutions that rely on algorithmic systems have significantly more agency and power over the lives of persons who come into their field of action.

But there is a further dimension of agency where a Christian perspective is relevant. Human agency is to be patterned on divine agency, specifically on the fact that there is a fundamental concordance between who God is and how God acts. This is often lacking in human beings and takes the form of hypocrisy and lack of integrity. Human agency thus conceived is therefore a call to act in such a way that our self and our actions match up. This will involve the capacity to offer a truthful account of our actions.[29] And it is precisely this capacity – a feature of our agency – which is being eroded today through design architectures that encourage impulsive, compulsive, and thoughtless action, such as "doom scrolling" or checking personal devices and social media feeds obsessively.[30]

Privacy as a proxy for human agency is clearly under assault today. As above, this can be seen in the use of "dark patterns" and manipulative "choice architectures " in user design (e.g. cookies policies that pop up upon visiting a website which encourage maximal surveillance), employed to "nudge" or "herd" people in a particular direction or incentivise a particular action. Ultimately, these tools reduce the ability for rational evaluation and, in the words of US Federal Trade Commissioner Rohit Chopra, "manipulate users into behavior that is profitable for an online service, but [is] often harmful to users or contrary to their intent".[31]

Moreover, the trajectory we are on, with massive investments being poured into brain-computer interfaces (BCIs), emotion recognition technology, the expansion of Virtual Reality (VR) and Augmented Reality (AR) technology assiduously hyped up by Meta under the "metaverse" brand[32], does not bode well for human agency and dignity.[33]

Of course, all of these developments warrant scrutiny in their own right. Suffice to say here that whatever these technologies may contribute to genuine human flourishing, in the logic of the surveillance system, they are also threatening to further undermine agency, and specifically the capacity for critical reflection and intentional action, but also the formation of virtuous habits such as care, temperance, patience, justice, and truthfulness.[34]

In an article published in December 2021 in *Wired* magazine, Oxford University philosopher and privacy expert Carissa Véliz tackles the question of freedom in the context of powerful algorithms that can predict human characteristics and behaviour with a high degree of accuracy.[35] In the piece, she deftly highlights the threat posed by AI-enabled hyper-personalisation of products and services (e.g. insurance premiums, mortgages, employment opportunities) to social cohesion and solidarity, the inadequate oversight for algorithmic decision-making systems, and the dangers of treating predictions about people, inferred from past data, as certainties about their future behaviour (e.g. predictive policing).

> **At the heart of our surveillance culture is a significant question: will we allow ourselves to be treated as mechanistic systems and stimulus-response automatons or as creatures with agency, dignity, and the freedom to defy odds and predictions about us?**

At the heart of our surveillance culture therefore is a deeply significant anthropological question: will we allow ourselves to be treated as mechanistic systems and stimulus-response automatons or as creatures with agency, inherent dignity, and the freedom (however conditioned and limited) to defy odds and predictions about us?

Human beings as embodied

A final feature of a Christian anthropology that is relevant for re-imagining privacy, and which follows on from the reflections above, is the embodied nature of human beings. Put simply, the human body is essential rather than secondary to personhood, a "feature not a bug" of what it means to be human. A concern for privacy is therefore a concern to preserve the dignity that attaches to being precisely the kind of embodied creatures that human beings are: with remarkable strength, resilience, and adaptability, but also limitations and susceptibilities. The latter are to be acknowledged and protected as essential features of being human rather than exploited for profit and unaccountable power.

> "
>
> **A concern for privacy is therefore a concern to preserve the dignity that attaches to being precisely the kind of embodied creatures that human beings are: with remarkable strength, resilience, and adaptability, but also limitations and susceptibilities.**

The previous section, on agency, implicitly pushed against deterministic accounts of what happens when humans engage with digital technology, even technology designed and optimised for maximising "engagement" and data collection. These tend to exaggerate the force of the technology in question on human agency to the point where they end up denying it. Here, a recognition of the vulnerability that comes with being embodied creatures, with limitations (physical, mental, emotional etc.), offers a strong foundation for resisting technologies and designs which exploit these vulnerabilities.

Concretely, what we should actively resist are designs and systems which manipulate and exploit our vulnerabilities and diminish our capabilities – for attention, for reflection, for deep and empathetic connection.[36] This will take the form of a combination of regulation, individual choice, and practice, as well as entrepreneurial responses in the form of digital technologies that put human wellbeing at the centre.

> **What we should actively resist are designs and systems which manipulate and exploit our vulnerabilities and diminish our capabilities – for attention, for reflection, for deep and empathetic connection.**

Moreover, if indeed our vulnerability is a feature of being human, a counter-intuitive source of strength rather than an embarrassment to be overcome, the trend towards ever increasing augmentation is to be seen as a threat to human dignity. Similarly, if physicality is fundamental to being human, our bodies connecting us to other creatures and the rest of the material world, the accelerating trend towards full immersion in virtual worlds (i.e. the metaverse) should be resisted for going against our nature as embodied creatures, and therefore seen as dehumanising.

[1] http://fra.europa.eu/en/charterpedia/article/1-human-dignity

[2] Shoshana Zuboff, "You Are the Object of a Secret Extraction Operation", *The New York Times,* 12 November 2021, https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html?fbclid=IwAR0sKVlu4aoB874Cy3mLD8bhAIK-ErkZjX-gce9a3_01_6bbZSx-lst4TM8

[3] See, for example, Margot Kaminsky, "Towards defining privacy expectations in an age of oversharing", *The Economist,* 16 August 2018. See also the relevant publications and initiatives of the Future of Privacy Forum (https://fpf.org), Privacy International (https://www.privacyinternational.org), and Amnesty International (https://www.amnesty.org/en/documents/pol30/1404/2019/en/)

[4] Patrick McGee, "Apple takes on the internet: the Big Tech battle over privacy", *Financial Times*, 30 April 2021, https://www.ft.com/content/3cabd134-0271-4783-8f0e-a17bb682afbe

[5] See, among others, Carissa Véliz, *Privacy is Power: Why and How You Should Take Back Control of Your Data* (London: Bantam Press, 2020)*;* Neil Richards, *Why Privacy Matters* (Oxford: Oxford University Press, 2021); Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, MA: Harvard University Press, 2018); Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge, UK: Cambridge University Press, 2018); Gry Hasselbalch, *Data Ethics of Power: A Human Approach in the Big Data and AI Era* (Cheltenham, UK: Edward Elgar Publishing, 2021).

[6] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles", https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[7] Daniel J Solove, "Understanding Privacy", Harvard University Press, May 2008, GWU Legal Studies Research Paper No. 420, GWU Law School Public Law Research Paper No. 420. Available at SSRN: https://ssrn.com/abstract=1127888. See also generally Daniel J Solove, "Conceptualizing Privacy", 90 CALIF. L. REV. 1087 (2002); Daniel J Solove, "A Taxonomy of Privacy", 154 U. PA. L. REV. 477 (2005).

[8] "Defining the Privacy Tech Landscape 2021", *The Rise of Privacy Tech*, November 2021, https://www.riseofprivacytech.com/definingprivacytechwhitepaper2021/

[9] Carissa Véliz, *Privacy is Power*.

[10] Evan Selinger and Woodrow Hartzog, "Obscurity and Privacy".

[11] Evan Selinger, "Stop Saying Privacy Is Dead", *Medium*, 11 October 2018, https://medium.com/s/story/stop-saying-privacy-is-dead-513dda573071

[12] Ari Ezra Waldman, "Privacy as Trust: Sharing Personal Information in a Networked World", 69 *University of Miami Law Review* 559 (2015). Available at SSRN: https://ssrn.com/abstract=2309632

[13] Neil M Richards and Woodrow Hartzog, "Privacy's Trust Gap", 126 *Yale Law Journal* 1180 (2017), Washington University in St Louis Legal Studies Research Paper 17-02-04. Available at SSRN: https://ssrn.com/abstract=2899760

[14] Helen Nissenbaum, "Privacy as contextual integrity", *Washington Law Review* 79(1) (2004), pp. 119-157.

[15] Notice-and-choice based on informed consent is the regulatory regime under GDPR. See "Woody Hartzog: Control is not the privacy solution it's made out to be", *IAPP*, https://iapp.org/news/video/woody-hartzog-control-is-not-the-privacy-solution-its-made-out-to-be/

[16] Ari Ezra Waldman, *Privacy as Trust,* p. 31.

[17] Ari Ezra Waldman, *Privacy as Trust*, pp. 32-33.

[18] See Daniel J Solove, "Understanding Privacy".

[19] Shoshana Zuboff, *The Age of Surveillance Capitalism*.

[20] For a detailed argument against turning autonomy into a governing value see Nathan Mladin and Stephen Williams, "Surveillance capitalism, autonomy, and the death of privacy", *Theos*, 7 October 2020, https://www.theosthinktank.co.uk/comment/2020/10/02/surveillance-capitalism-and-autonomy

[21] Emily Downe, "Nobody Stands Nowhere", *Theos*, 13 May 2021, https://www.theosthinktank.co.uk/comment/2021/05/12/worldviews-film

[22] "What Is Privacy?", *Privacy International*, 23 October 2017, https://www.privacyinternational.org/explainer/56/what-privacy

[23] Luciano Floridi, "On Human Dignity and a Foundation for the Right to Privacy" (26 April 2016). Available at SSRN: https://ssrn.com/abstract=3839298

[24] "Reflections on AI: Q&A with John Tasioulas", *YouTube*, https://www.youtube.com/watch?v=BkL912amlTs&t=4s

[25] L M Sacasas, "Perspectives on Privacy and Human Flourishing", *Second Nature*, 21 April 2014, https://secondnaturejournal.com/perspectives-on-privacy-and-human-flourishing/

[26] I am grateful to L. M. Sacasas for this insight.

[27] To avoid ableism, this capacity should be understood in accordance with the condition or stage in life of any given person. A severely disabled person's capacity for thinking, feeling, and acting in the world should not be measured against the same capacities of an able-bodied person, but uniquely, in a qualified way, according to their condition. In some cases, a person's capacity for action will be limited to their sheer presence, and that will suffice. Embodied presence, in this case, should be considered an expression of agency.

[28] I am grateful to Michael Burdett for this insight.

[29] I am grateful to Matt Prior for this insight.

[30] See Stanley Hauerwas, *The Work of Theology* (Grand Rapids, MI: Eerdmans, 2015), Chapter 4: "How to be an Agent: Why Character Matters". I am grateful to Matt Prior for this reflection.

[31] "Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning", *USA Federal Trade Commission*, 2 September 2020, https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf

[32] Broadly defined, the metaverse is a set of computer-generated, network-extended spaces (XR, which includes VR, AR, and/or MR) in which interactions take place among humans and automated entities, some in gaming worlds and some in "mirror worlds" that duplicate real-life environments.

[33] See, for example, Kate Wild, "'Our notion of privacy will be useless': what happens if technology learns to read our minds?", *The Guardian*, 6 November 2021, https://www.theguardian.com/technology/2021/nov/07/our-notion-of-privacy-will-be-useless-what-happens-if-technology-learns-to-read-our-minds and "UN Human Rights Council adoption of 'Right to privacy in the digital age': Emotion recognition technologies acknowledged", *Emotional AI Lab*, 25 October 2021, https://www.emotionalai.org/news/2021/10/25/un-human-rights-council-adoption-of-right-to-privacy-in-the-digital-age-emotion-recognition-technologies-now-an-emergent-priority

[34] Sigal Samuel, "It's hard to be a moral person. Technology is making it harder", *Vox*, 3 August 2021, https://www.vox.com/the-highlight/22585287/technology-smartphones-gmail-attention-morality. See also Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting* (Oxford, UK: Oxford University Press, 2016)

[35] Carissa Véliz, "If AI Is Predicting Your Future, Are You Still Free?", *Wired*, 27 December 2021, https://www.wired.com/story/algorithmic-prophecies-undermine-free-will/

[36] On these themes, see Sherry Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other* (New York, NY: Basic Books, 2011) and Sherry Turkle, *Reclaiming Conversation: The Power of Talk in a Digital Age* (New York, NY: Penguin Press, 2015).

Conclusion

This essay has tried to describe what is by now a familiar narrative about the intersection of digital technology, especially cutting-edge machine learning algorithms, Big Data and Big Tech firms – what is commonly discussed under the rubric of surveillance capitalism or the data economy. Chapter 1 described the surveillance system and sought to explain its workings. The next two chapters focused on three case studies where the dynamics of digital surveillance are worked out and where most of the public concern has tended to gravitate: social media, the use of facial recognition technology, and predictive policing. The final chapter offered a broader vision of privacy – one of the key concerns and values threatened by the surveillance system.

Despite its elusiveness, the term privacy continues to have currency and encapsulate many of the concerns people have with the workings and direction of the surveillance system. The last chapter tried to place privacy on a more robust, indeed truer anthropological footing. The vision of privacy I put forward in this essay is one rooted in personal dignity – that is, the dignity and value of being precisely the kind of creatures that we are. Drawing on theological anthropology, I highlighted three key features of being human that were relevant to our discussion:

- *Relationality*. We are fundamentally relational creatures, persons-in-relationship not simply individuals – the implication being that an approach to these issues that is based on an individualist conception of the human person, and a strictly rights-based approach to privacy are insufficient.

- *Agency*. We are creatures with agency or the potential for it. I defined agency not in terms of autonomy, but as the capacity to think, feel, and act in a self-directed way, according to one's condition, without unwanted intrusion and interference. The first implication of this is that determinist accounts of individuals interacting with technology, where humans are entirely subordinate to, and even at the mercy of, technology, are false and detrimental. The second implication is that technologies designed and deployed to erode human agency, for example through various forms of algorithmically driven nudging, are antithetical to personal dignity and ultimately dehumanising.
- *Embodiment*. Finally, I noted that theological anthropology assumes that human beings are *fundamentally embodied creatures*. Bodies are constitutive rather than incidental to personhood. The upshot here is that technologies which exploit human vulnerabilities and weaknesses (in the form of addictive and manipulative design, for example) but also technologies underpinned by transhumanist philosophy and based on a practical disdain for the body, leading to increasing abstraction from the body and embodied existence in the physical world, should be resisted.

One of the most common ways activists and academics concerned with the surveillance economy frame their concerns is in terms of remedying the wide and indeed growing power disparities between, on the one hand, individuals, and corporates and state agencies, on the other.

Indeed, power is a valid and important lens on the subject, bound up with the notion of agency. More significant still is protecting human dignity. As Chapter 4 has tried to show, dignity should be understood as the value of being precisely the kind of creatures that human beings are: *fundamentally relational*, *embodied,* and *with agency or the potential for it.*

To this end, there are regulatory reforms to support as well as individual choices to be made. The latter include rejecting default settings on websites, apps, and devices, that generally seek maximal data collection; obfuscatory tactics to interrupt the unaccountable data harvesting practices[1], and use of privacy-conscious technologies and services, including privacy-friendly search engines (e.g. DuckDuckGo, Brave) and email providers (e.g. ProtonMail).[2]

As for systemic responses, the proposal to ban all commercial activity involving personal data, and effectively end the data economy altogether, has little traction in contemporary debates, though it should be seriously considered.[3] Encouragingly, there is growing momentum behind tighter regulation of the Big Tech sector. At least 48 countries introduced rules relating to data, advertising, content, or competition regulation in 2021 alone.[4] While there are differences in emphasis between countries, the regulatory responses converge around bolstering verifiable transparency, accountability, and responsibility with regard to data and algorithms.[5] Researchers and regulators should be given access to data and algorithms, including proprietary ones, to this end.[6]

In addition to these national efforts, there are also a wide set of supra-national and multi-stakeholder initiatives on regulating Big Tech, AI, and the data economy, most notably the legislation and proposals drafted by the EU under President Ursula von der Leyen's leadership: ePrivacy Directive, Artificial Intelligence Act, the Digital Services Act, the Digital Markets

Act, and the Data Governance Act under the umbrella of an overarching Digital Strategy. The UK is also set to release the final draft of its own Online Safety Bill, and the Office for Artificial Intelligence is expected to release a white paper on governing and regulating AI.

But while these regulatory developments are welcome and necessary and promise to address many of the concerns raised throughout this essay, they are unavoidably insufficient. Time and again, technology outruns regulation. With AI, this is even more so the case. What is needed is, on the one hand, human-centred innovation and product design. But the question arises: whose conception of the human should guide these "supply side" solutions? As this essay has tried to show, theological anthropology should be seen as a rich source of wisdom to draw on. Especially if what we seek is a rounded, rather than reductionist, a realistic, rather than an idealised, understanding of the human person.

But humane technology and robust regulation alone or indeed together are still not enough. To believe the contrary is to buy into the false notion that all our social and political ills are merely "problems" in search of the right solution. Call this the technocratic and technosolutionist fallacy.[7] The crisis of our democracies and deepening polarisation of public opinion, for example, is not simply a function of badly designed and poorly regulated social platforms. The causes are legion. The responses should be too. Among them, two worth mentioning in closing are the sustained cultivation of friendship across ethnic, religious, social, and political divides, and participation in embodied communities of hospitality and virtue.[8] As technology races forward, these are crucial disciplines which contain the seeds of hope for healing our democracies and reweaving our common life.

[1] See, for example, Finn Brunton and Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (Cambridge, MA: MIT Press, 2015).

[2] See also the Center for Humane Technology's "Take Control of Your Social Media Use" toolkit: https://www.humanetech.com/youth/take-control-of-your-social-media-use

[3] "Time to ban surveillance-based advertising: The case against commercial surveillance online", *Forbruker Radet,* June 2021, https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf.

[4] Adrian Shahbaz and Allie Funk, "Freedom On the Net 2021: The Global Drive to Control Big Tech", *Freedom House*, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech#Regulation

[5] See also the UNESCO "Recommendation on the Ethics of Artificial Intelligence", which is the first global normative framework on AI ethics: https://unesdoc.unesco.org/ark:/48223/pf0000379920#page=14

[6] Tara Wright, "The Platform Transparency and Accountability Act: New legislation addresses platform data secrecy", *Cyber Policy Center, Stanford University*, 9 December 2021, https://cyber.fsi.stanford.edu/news/platform-transparency-and-accountability-act-new-legislation-addresses-platform-data-secrecy

[7] Writing in *The Hedgehog Review*, Christine Rosen describes technosolutionism as "a way of understanding the world that assigns priority to engineered solutions to human problems. Its first principle is the notion that an app, a machine, a software program, or an algorithm offers the best solution to any complicated problem. Notably, the technosolutionist's appeal to technical authority, even for the creation of public policy or public health measures, is often presented as apolitical, even if its consequences are often not." See "Technosolutionism Isn't the Fix", https://hedgehogreview.com/issues/america-on-the-brink/articles/technosolutionism-isnt-the-fix

[8] L M Sacasas, "The Skill of Hospitality", *Breaking Ground*, 13 November 2020, https://breakingground.us/ivan-illich-technology-skill-of-hospitality/

Theos – enriching conversations

Theos exists to enrich the conversation about the role of faith in society.

Religion and faith have become key public issues in this century, nationally and globally. As our society grows more religiously diverse, we must grapple with religion as a significant force in public life. All too often, though, opinions in this area are reactionary or ill informed.

We exist to change this

We want to help people move beyond common misconceptions about faith and religion, behind the headlines and beneath the surface. Our rigorous approach gives us the ability to express informed views with confidence and clarity.

As the UK's leading religion and society think tank, we reach millions of people with our ideas. Through our reports, events and media commentary, we influence today's influencers and decision makers. According to *The Economist*, we're "an organisation that demands attention". We believe Christianity can contribute to the common good and that faith, given space in the public square, will help the UK to flourish.

Will you partner with us?

Theos receives no government, corporate or denominational funding. We rely on donations from individuals and organisations to continue our vital work. Please consider signing up as a Theos Friend or Associate or making a one off donation today.

Theos Friends and Students

- Stay up to date with our monthly newsletter
- Receive (free) printed copies of our reports
- Get free tickets to all our events

£75/ year
for Friends

£40/ year
for Students

Theos Associates

- Stay up to date with our monthly newsletter
- Receive (free) printed copies of our reports
- Get free tickets to all our events
- Get invites to private events with the Theos team and other Theos Associates

£375/ year

Sign up on our website:
www.theosthinktank.co.uk/about/support-us

Recent Theos publications include:

The Nones: Who are they and what do they believe?
Hannah Waite

A Torn Safety Net: How the cost of living crisis threatens its own last line of defence
Hannah Rich

'Science and Religion': Moving away from the shallow end
Nick Spencer and Hannah Waite

Valuing Women: Making women visible
Kathryn Hodges

Beyond Left and Right: Finding Consensus on Economic Inequality
Hannah Rich

Just Work: Humanising the Labour Market in a Changing World
Paul Bickley

Relationships, Presence and Hope: University Chaplaincy during the COVID-19 Pandemic
Simon Perfect

The Church and Social Cohesion: Connecting Communities and Serving People
Madeleine Pennington

Data and Dignity
Why Privacy Matters in the Digital Age

It's becoming old news: we are continually tracked, analysed, and profiled by private companies and governmental agencies. Our data is hoovered up and used to predict and manipulate our behaviour. A new cultural and economic order is here: surveillance capitalism or what this essay calls the 'surveillance system'.

Of the many concerns raised, privacy is never far from the top. But what is privacy? Most often, it's described as an individual's right to control their data. But this is not enough. If it is to serve us well in resisting dehumanising uses of technology, privacy must be re-imagined.

Drawing on Christian thought, although anticipating overlap with other religious or philosophical traditions, this essay sketches a conception of privacy centred on the notion of dignity and based on the sort of creatures human beings are: *embodied* (with limits and susceptibilities to be honoured rather than violated for gain), *relational* (made for relationships of trust and mutual care rather than exploitation), *agential* (with a capacity for intentional action to be upheld rather than undermined).

Privacy is not dead, nor should it be allowed to die. Privacy is a form of neighbour love in the digital age.

Nathan Mladin is a Senior Researcher at Theos. He is the author of several Theos publications and has previously written on surveillance and privacy in *The Robot Will See You Now: Artificial Intelligence and the Christian Faith* edited by John Wyatt and Stephen Williams (SPCK, 2021). Nathan holds a PhD in Systematic Theology from Queen's University Belfast.

Cover image: Mati Mango via Pexels.com