

Risk and Surveillance Capitalism

Margaret McGaley

Margaret McGaley completed her PhD in Computer Science on the topic of e-voting in 2008. She founded Irish Citizens for Trustworthy Evoting in 2003, which was instrumental in the successful campaign against the use of a dangerous e-voting system in Irish elections. She appeared as an expert before a joint oireachtas committee in 2003, and the South African Independent Electoral Commission in 2013. She lives on a permacultural smallholding in Tipperary.

Introduction

People are notoriously bad at assessing risk - we instinctively overestimate the likelihood of very scary events and underestimate the likelihood of familiar hazards.¹ When this is combined with the power of gradual change, we end up collectively accepting situations that we would never rationally choose. The motorcar is the classic example: if we could objectively weigh the advantages (fast, autonomous personal transport) against the disadvantages (high risk of personal injury/death, environmental pollution, stress, dedicating large tracts of land to sole use of cars, etc.) we would likely come up with a very different system.

The modern Internet is another excellent example of our failure to assess and respond to risk. Discussions about risk and the Internet are often individualistic: What if my credentials are stolen? What if my search history is revealed? But we ought to be concerned about the wider impact. Our individual choices—however minor—add up to collective action.

Smartphones, social media, the Internet of Things: these tools have been broadly integrated into our lives with very little oversight. How are they changing our society? What risks have we (unwittingly) taken on with their adoption? Who is driving the change, and how do their priorities and incentives line up with those of broader society?

Our data is being collected in ways that were inconceivable 20 years ago. Indeed, the idea of “personal data” would have been irrelevant to most people then. This technological shift has brought about tremendous social, political, and economic changes which are still being processed: for example, in our attitudes to privacy, citizenship, and work. In this essay, I want to explore the digital transformation of capitalism and how it introduces a range of risks that could not have been imagined before the development of the Internet.

¹ Morgan Housel. "Why We're Awful at Assessing Risk." *USA Today*. March 17, 2014. <https://eu.usatoday.com/story/money/personalfinance/2014/03/17/why-were-awful-at-assessing-risk/6530753/> The International Standards Organization defines risk as the “effect of uncertainty on objectives” (ISO 31000). Risk analysis is an important field in Computer Science which aims to overcome cognitive biases to analyse risks more objectively. To make comparisons, risks are often analysed as the combination of the likelihood of a hazard with the severity of its effects.

Privacy

We are all influenced by the old maxim "if you have done nothing wrong you have nothing to hide", inclined to think that we're too small to be interesting. Like dead skin cells, we spend our days shedding data.. Almost invisible, but it adds up to a lot of dust.²

Individually, perhaps we are too small to be interesting, but our collated data reveals things that leave us open to manipulation. And in reality, we all do have something to hide. Firstly, we all *have* done something wrong, but we also organise surprises for loved-ones, or ponder questions that would be embarrassing or awkward if made known. Many of us have (for example) political opinions, family history, or medical history that could conceivably be used against us.

Privacy is also analogous to vaccination. National immunisation programs provide "herd immunity": illnesses cannot take hold and reach epidemic levels, because so many members of the community are immune. Vulnerable people (for example those with suppressed immune systems) are protected because of the actions of the group. Similarly, a general expectation and protection of privacy is important for specific individuals who *are* interesting, such as whistleblowers and journalists. If Edward Snowden had not been able to act in secret, he could not have made the revelations that he did. There are other marginalised groups, whose race, gender, or non-mainstream lifestyles make them targets for bullying and harassment.³ By protecting everyone's freedom to act in a reasonable amount of secrecy, we protect those who require secrecy to resist oppression. And so we all benefit, and we protect vulnerable members of our society. Solidarity with the marginalised is a way of preserving the common good.⁴

The powerful have always dreamed of controlling the masses by close supervision, but it has never been such a realistic prospect as it is today. The new reality is that corporations have the means and the incentives to extrapolate a great deal of our internal state from the trail of data we leave as we surf. It has become a common occurrence to see an ad and think "how do they know I want that?"⁵

² In 2017, Andre Buxey undertook a small experiment to see how many cookies he would generate in a typical day. He developed a fairly minimum 'typical browsing day' of 57 unique URLs. The total tally of cookies this generated was 826, most of which were for ad serving networks. Andre Buxey. "How Many Cookies Do You Collect on an Average Day?" *Rogerwilco*. September 6, 2017.

<https://www.rogerwilco.co.za/blog/how-many-cookies-do-you-collect-average-day>. NPR has a very accessible conversation about data-collection on their Fresh Air program: Davies, Dave. "How Tech Companies Track Your Every Move And Put Your Data Up For Sale." *NPR*. July 31, 2019.

<https://www.npr.org/2019/07/31/746878763/how-tech-companies-track-your-every-move-and-put-your-data-up-for-sale?t=1566300386455>. Nick Statt. "Google Has Been Tracking Nearly Everything You Buy Online - See for Yourself with This Tool." *The Verge*. May 17, 2019.

<https://www.theverge.com/2019/5/17/18629789/google-purchase-history-gmail-email-receipts>

³ Representatives of these groups are always among the first to call out the tech giants on the privacy implications of their services. Nitasha Tiku. "Three Years of Misery Inside Google, the Happiest Company in Tech." *Wired*. August 16, 2019. <https://www.wired.com/story/inside-google-three-years-misery-happiest-company-tech>. It should be noted that religious groups already are or will in the future be included in these marginalised groups.

⁴ From a Jesuit perspective, this seems to be implied in the trajectory of the most recent General Congregation of the Society of Jesus. See especially the concluding paragraph of Decree 1. Society of Jesus, "Decree 1: Companion in a Mission of Reconciliation and Justice" in *General Congregation 36 Decrees and Documents* (Dublin: Messenger, 2017), §40, 39.

⁵ A very early comment on the phenomenon comes from this satirical piece: "Amazon.Com Recommendations Understand Area Woman Better Than Husband," *The Onion*, September 1, 2007,

It is unlikely that this is a result of direct surveillance of your conversations, but neither is it a coincidence. In fact, you have left behind such a detailed web of data that algorithms can predict your desires. This is much, much worse.

At the same time, it is ever more difficult to live in the modern world without interacting with data-hungry websites. Social groups typically organise themselves on one of the big proprietary social media platforms. Therefore, the decision to not sign up isolates oneself. Almost every website is collecting huge amounts of data through technologies like cookies and Internet Protocol⁶ geolocation. The requirements introduced by the General Data Protection Regulation have highlighted the extent of this reality for many people, but hardly solved the problem.

Since mid-2019, almost anyone who applies for a US visa will be required to provide their social media usernames. If you've chosen not to use those websites because you don't trust them, you risk looking abnormal, and thereby suspicious.⁷

Smartphones offer amazing convenience, and social networks offer feelings of connectedness in an increasingly lonely world. The average smartphone user has a limited understanding of computer security. The average software developer has a limited sense of responsibility for the moral and ethical implications of their work.⁸ It can be more lucrative for corporations to play fast and loose with data. These factors have resulted in software that offers inadequate protections, and an erosion of our expectations of privacy online.

It is interesting to see what happens when an individual tries to challenge these new privacy norms. In 2013, Janet Vertesi decided to keep her pregnancy secret from the algorithms.⁹ No doubt she had many reasons for this decision, but as a sociologist of technology, one of them was scientific curiosity as to whether it was even possible. Her attempts to maintain her privacy often looked suspicious. When her husband tried to buy a large number of gift cards (in an attempt to anonymize their purchase of a buggy) he was confronted by a notification stating that the store "reserves the right to limit the daily amount of prepaid card purchases and has an obligation to report excessive transactions to the authorities."

Our everyday choices are being closely observed and their implications analysed. And it is rapidly leading to a situation where attempting to protect your privacy looks like criminal activity.

<https://www.theonion.com/amazon-com-recommendations-understand-area-woman-better-1819568885>

⁶ The Internet protocol address is a unique numerical label assigned to each device connected to a computer network that uses the internet for communication.

⁷ David Millward. "The US Now Wants to Check Travellers' Social Media - and It's Going to Cause Chaos." *The Telegraph*. June 05, 2019. <https://www.telegraph.co.uk/travel/news/us-visa-social-media-handles/>

⁸ Laura Nolan. "INOG::12 (3) On the Ethical Crisis in Technology." *YouTube*. March 06, 2019. <https://www.youtube.com/watch?v=cW3bO8XluH0>

⁹ Janet Vertesi. "Internet Privacy and What Happens When You Try to Opt Out." *Time*. May 01, 2014. <https://time.com/83200/privacy-internet-big-data-opt-out/>

Citizenship

Every day we voluntarily hand over information that previous generations recognised the need to guard, but who are we handing it to? Over the last few decades there has been a shift from government surveillance to surveillance by private enterprises, and where governments *are* undertaking digital surveillance, they are often outsourcing it to private companies.¹⁰

Governments, at least nominally, act in the public interest. In modern liberal democracies, governments are expected to justify their actions in terms of the public good. Companies are not bound by such requirements; their primary responsibility is to their shareholders, including venture capitalists.

It is companies who are collecting and analysing every scrap of information they can about us. They are not doing it for ideological reasons: they are doing it to maximise profit, in part to play on our fears and sell us “solutions.” They are not subject to oversight in the way that public and academic bodies are. There are rarely ethics committees deciding whether their experiments are acceptable and where such oversight does exist, its remit is to serve the corporation’s best interests, which reduces to profit.

We have known for generations that the human mind is frighteningly hackable; bad actors with the required knowledge and access can (in limited, but significant ways) make us think and feel things that they choose.¹¹ The ubiquity of smart devices, and the extent of the access we have granted them to our lives has led to unprecedented vulnerability to these techniques, both in terms of the number of people and the degree of access.¹² And of course the large number of potential victims involved allows for selection of those most susceptible.

Cambridge Analytica have been accused of interfering in the electoral process in Trinidad (among other places). While the truth of such claims remains to be settled, it is a plausible story. It is conceivable that a bad actor with sufficient data and enough people’s attention could alter the outcome of an election.¹³

¹⁰ Famously, Edward Snowden was working for one such firm sub-contracted to enact surveillance, Booz Allen Hamilton, when he prepared his leaks. Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (New York, NY: Metropolitan Books, 2014), 84.

¹¹ Think of Socrates’ dialogue with Gorgias about the nature of rhetoric as the art of inducing “belief without knowledge.” Plato, *Gorgias* (London: Penguin Classics, 2004), 16.

¹² Georges Abi-Heila. “Ads Just Work, No Matter What You Think.” <https://hackernoon.com/nobody-is-immune-to-ads-7142a4245c2c>.

¹³ While the exact potency of the technology remains up for debate, the influence of the firm Cambridge Analytica, working through the Facebook network, on some of the most contentious elections of recent history is a noteworthy and alarming example. Carole Cadwalladr, and E. Graham-Harrison. “The Cambridge analytica files.” *The Guardian* 21 (2018): 6-7.

Science fiction has long predicted the replacement of elected government by for-profit corporate power. Mega-corporations that war with each other through trade, espionage, and violence, unfettered by elected government, have featured in many a cyberpunk novel.¹⁴ As time goes on, these scenarios are seeming less and less fanciful. European governments have ceded a lot of power, and abdicated a lot of responsibility, through privatisation since the 1980s. That trend continues with outsourcing. Trans-national corporations are—if not dictating—heavily influencing public policy around the world.¹⁵ Governments are outsourcing their functions so that private companies are becoming the de-facto arbiters in law-enforcement, education, and health-care (among other things).

It is all too easy to imagine a kind of New Feudalism, in which our status as consumers and employees is more important than our status as citizens.¹⁶ And God help those who cannot get a prestigious job, or afford the right purchases.

The advertising industry is at the heart of the modern web.¹⁷ The spread of Internet access beyond military and university use came at a time when the provision of public utilities as a public good was being replaced by privatisation in the name of competition and efficiency. There was never any question that the Internet must be self-sustaining financially. While there are some websites with successful subscription models, it is undeniable that the majority of the money changing hands is paying for attention in the form of advertising.

In order to “target” ads, websites and platforms collect as much data as possible about individual users, and categories of users. The advertising industry has earned a reputation for ruthlessness. There’s no reason to believe they would hesitate to use amoral practices in analysing and deploying such data.

The advent of the Internet of Things (IoT) is extending privacy breaches and de-facto corporate power further into the “real world.”¹⁸ Media headlines about data concerns abound: landlords

¹⁴ For the impact of science fiction literature on the political imagination, consider Will Davies (ed.), *Economic Science Fictions*, (London: Goldsmiths Press, 2014).

¹⁵ Jeva Lange, "Mark Zuckerberg Confirms Facebook Decided on Its Own to Ban Foreign Pro-life Ads in Ireland Ahead of Referendum Vote," *The Week*. June 26, 2019. <https://theweek.com/speedreads/849472/mark-zuckerberg-confirms-facebook-decided-ban-foreign-prolife-ads-ireland-ahead-referendum-vote>

¹⁶ This is a major theme in the important work of Evgeny Morozov. See for example: Evgeny Morozov, *To Save Everything, Click Here* (London: Penguin, 2013) or for an online example: Evgeny Morozov, "Google's Plan to Revolutionise Cities Is a Takeover in All but Name," *The Guardian*, October 21, 2017. <https://www.theguardian.com/technology/2017/oct/21/google-urban-cities-planning-data>

¹⁷ Morozov is very strong on this point. His discussion of how algorithms exploit what they can tell about our interests to sustain attention for the sake of advertising is alarming. Morozov, 161-162.

¹⁸ Any serious engagement with policy around technology must begin by recognising the world wide web is the “real world” and not some virtual zone of depleted significance or relevance. One can lament the influence of social media, of the dark web, or whatever technological development you choose, but it is no longer viable for those involved in Irish policy-making to imagine that it is something that can be ignored.

requiring all of their tenants to use insecure “smart” locks,¹⁹ deals struck between police forces and manufacturers of “smart” home security systems,²⁰ facial recognition software being used on CCTV footage from the London Underground,²¹ or even at football matches.²² But in an atmosphere of fast-paced “disruption” very little seems to be done about it. As computer professionals like to joke: the “s” in IoT stands for “security”.

Of course, we would not want to overestimate the competence of these companies. To quote Maciej Cegłowski “... this talk of secret courts and wiretaps is a little bit misleading. It leaves us worrying about James Bond scenarios in a Mr. Bean world.”²³ But if the owners of these vast databases are not handling them competently, then they are handling them incompetently. I’m not sure which is worse.

The ideal of a State where every individual has equal value and power is really not that old, and it certainly hasn’t been achieved yet, but it is well on its way to seeming quaint.

Work

The automation of human work has been accelerating since the dawn of the industrial revolution, if not before. Somehow, instead of increasing leisure time for everyone, those who have work are working longer and more intensely.²⁴

The advent of modern artificial intelligence (AI) promises—or threatens—to automate areas of work never before imagined susceptible.²⁵ But these AI systems are not the impartial truth-tellers that some would have us believe. They are, in Cegłowski’s words “like money laundering for bias”.²⁶ They embed prejudice and inequality behind an implacable “computer says “no”,” while accumulating the wealth that formerly supported the people doing the work.²⁷

¹⁹ MalwareTech. "After 1 Hour of Looking at My New Smart Lock, I Am Now Able to Remotely Unlock Every Front Door in the Apartment Complex." *Twitter*. August 12, 2019.

<https://twitter.com/MalwareTechBlog/status/1160845561035153408>

²⁰ Caroline Haskins. "Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement." *Vice*. July 25, 2019. https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement

²¹ Madhumita Murgia. "London's King's Cross Uses Facial Recognition in Security Cameras." *Financial Times*. August 12, 2019. <https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c>

²² Maya Wolfe-Robinson, "Manchester City Warned against Using Facial Recognition on Fans," *The Guardian*, August 18, 2019, sec. Technology, <https://www.theguardian.com/technology/2019/aug/18/manchester-city-face-calls-to-reconsider-facial-recognition-tech>

²³ Maciej Cegłowski. "The Internet With A Human Face - Beyond Tellerrand 2014 Conference Talk." May 20, 2014. https://idlewords.com/talks/internet_with_a_human_face.htm

²⁴ Peter Fleming’s discussion of the “endlessness” of contemporary work is a rich and psychologically sensitive account of this intensification. Peter Fleming, *The Mythology of Work* (London: Pluto Press, 2015), 49-58.

²⁵ See: Rutger Bregman, *Utopia for Realists* (London: Bloomsbury, 2016), 177-200.

²⁶ Maciej Cegłowski. "Remarks at the SASE Panel On The Moral Economy of Tech." June 26, 2016. https://idlewords.com/talks/sase_panel.htm

²⁷ Cathy O’Neil, *Weapons of Math Destruction* (London: Penguin, 2017).

As more and more of the productivity encompassed by Gross Domestic Product is produced by machines, the labour that can only be performed by human beings is becoming restricted to care work (which has always been undervalued within capitalism²⁸) and the production of the data on which the algorithms depend.

If we are going to insist that profits be distributed by contribution, rather than need, we must begin to consider ways to compensate people for their production of data.²⁹ Since these AI systems are completely dependent on inconceivably huge datasets, a strong analogy exists here with mining.³⁰ There have been countless examples of communities in possession of natural resources, but no means to exploit them, who therefore received completely inadequate compensation from those who funded the digging. Artificial intelligence systems are as dependent on our data as the industrial revolution was on steel. To avoid the rampant inequalities of the first industrial revolution, this digital industrial revolution requires a new approach to sharing profits.

It can be hard for the lay-person to understand just how much information can be gleaned from a large enough database. Here is a small example: imagine an AI that had access to anonymised³¹ credit card histories. It could reveal that two credit-card users spent the weekend together, by discovering a series of pairs of transactions where the two cards were used in quick succession. Machine-learning algorithms are capable of analysing very, very large amounts of data and discovering patterns we could never have found. That data is key: they cannot function without it, and they cannot produce it.

The advent of high-speed communication technologies is also negatively impacting workers in another way, through the so-called 'gig-economy'. Companies dole out work, piecemeal. They claim to be 'disrupting' markets but often they are side-stepping regulations which were introduced to protect workers.³²

If we allow the process discussed in the previous section—that is, the transfer of political power from elected governments to profit-making organisations—then we have no reason to expect a humanitarian solution to the burgeoning employment crisis. There is an argument that says the system requires consumers to function, and therefore the market will demand that consumers have the means to make purchases. We must recognise the risk entailed in trusting this as the basis of our collective response to the problem.

²⁸ Kathi Weeks, *The Problem of Work* (Durham, NC: Duke University Press, 2011).

²⁹ Hart, Vi. "Changing my Mind about AI, Universal Basic Income, and the Value of Data". *The Art of Research*. May 31, 2019. <https://theartofresearch.org/ai-ubi-and-data/>

³⁰ Abeba Birhane. "The Algorithmic Colonization of Africa." *Real Life*. July 18, 2019. <https://reallifemag.com/the-algorithmic-colonization-of-africa/>

³¹ Alex Hern. "'Anonymised' data can never be totally anonymous, says study". *The Guardian*. 23 Jul 2019. <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds>

³² Hena Matthias. "Problems Within the Gig Economy." *IONA Journal*. February 26, 2019. <https://www.ionajournal.ca/exchange/2019/2/25/problems-within-the-gig-economy>

Work done by humans is subject to scrutiny in a way that work done by computers does not seem to be. There may be many psycho-socio-historical reasons for this, but among them is a pervasive belief in the objectivity of computers; an idea that they follow logic relentlessly, that their conclusions have a kind of mathematical purity. In fact, computers can only do exactly what they are told to do, whether or not the programmer understands what that is. As the old computer-science aphorism goes: garbage in, garbage out. The AIs that are being developed as part of this automation revolution will not overturn prejudice and systemic injustice unless we figure out how to tell them to.

The Irish Context

We need look no further than the introduction of the Public Services Card for an example of a system that poses a potential surveillance threat, which has been introduced in a haphazard way.³³ It could well be that a national identity card, tied to a secure database containing medical records and similarly sensitive information, would be worth having. If we were to carefully examine the trade-offs between privacy and convenience, we might choose convenience. But that is not a debate which has been undertaken. Instead the government has tried to introduce the card using stealth and threats,³⁴ for unclear motives,³⁵ and without adequate security measures.³⁶

The card was introduced on a pilot basis in 2011, and the process of rolling it out across the nation began the following year. The order in which demographics were required to register for the card arguably targeted “groups who traditionally don’t have a particularly loud voice in the public sphere.”³⁷ By 2017, Minister for Public Expenditure, Pascal Donohoe, was still claiming that the card was voluntary,³⁸ despite the growing list of “consequences for not volunteering”³⁹ (including having social welfare payments cut off, being unable to get a new driver’s licence, or replace a lost or stolen

³³ An Coimisiún um Chosaint Sonraí, “DPC Statement on Matters Pertaining to the Public Services Card,” Data Protection Commission, August 16, 2019, <https://www.dataprotection.ie/dpc-statement-matters-pertaining-public-services-card-0>.

³⁴ Consider the confusion around whether biometric data was being processed: Elaine Edwards, “‘Augmented Identity’ Firm Gets €9m Contract for Public Services Cards,” *The Irish Times*, July 5, 2018, <https://www.irishtimes.com/news/ireland/irish-news/augmented-identity-firm-gets-9m-contract-for-public-services-cards-1.3555710>.

³⁵ Citizens often found themselves asking, “but why?” when faced with the “whole load” of purposes to which the card was to be put. Cianan Brennan, “Pretty Soon You’re Going to Need This Card to Do a Whole Load of Important Things in Ireland - but Why?,” *TheJournal.ie*, July 15, 2017, <https://www.thejournal.ie/public-services-card-3496359-Jul2017/>.

³⁶ Simon McGarr. “The Public Services Card- The ID Card That Reveals the Irish State’s Id.” August 23, 2017. <https://www.mcgarrsolicitors.ie/2017/08/23/public-services-card-id-database-id-card/amp/>

³⁷ Loughlin O’Nolan, and Elaine Edwards. “The Identity Card That Most Assuredly Isn’t An Identity Card.” May 30, 2017. <http://myprivacykit.com/projects/the-identity-card-that-most-assuredly-isnt-an-identity-card/>

³⁸ Mark Hilliard. “Public Service Card Use Not Mandatory, Says Donohoe.” *The Irish Times*. March 23, 2017. <https://www.irishtimes.com/business/technology/public-service-card-use-not-mandatory-says-donohoe-1.3022649>

³⁹ Simon McGarr. “The Public Services Card- The ID Card That Reveals the Irish State’s Id.” *McGarr Solicitors Blog* August 23, 2017. <https://www.mcgarrsolicitors.ie/2017/08/23/public-services-card-id-database-id-card/amp/>

passport, or even to get your first passport or become a citizen). There were a number of red-flags raised by the project including a lack of transparency, a push to force uptake rather than making the card genuinely attractive to potential users,⁴⁰ and scope creep.⁴¹

Simon McGarr, a solicitor who has been a gadfly⁴² to successive Irish governments on several important topics,⁴³ spent a lot of time challenging the introduction of the card,⁴⁴ but it was the mistreatment of a pensioner that really pushed the problems with the card into the light.⁴⁵ Her pension had been withheld for 18 months because she refused to register for the card unless and until she was shown proof that it was a legal requirement.

This card is just the latest in a long list of IT projects where the Irish government have failed to evaluate risk before pushing forward with ill-conceived systems: Pulse, PPARS⁴⁶, e-voting, and the Public Services Card all betray a deep failure to understand the complexity of, and risks associated with, modern technology. In each case, genuine concerns voiced by informed members of the Irish public were dismissed as scare-mongering. In each case, reality dawned gradually. But the Irish state has still not learned how to procure high-quality IT systems that provide adequate security safeguards for citizens' private data.⁴⁷

Conclusion

Shoshanna Zuboff has coined the phrase “surveillance capitalism” to describe the context discussed in this essay. Her definitive book on this topic⁴⁸ is an eloquent survey of the history and implications

⁴⁰ Ibid.

⁴¹ Scope creep is a common phenomenon in mismanaged IT projects. It is the tendency for new features, beyond the intended scope of the project, to be added haphazardly during development. It is distinct from modern ‘agile’ software development practices, which manage project scope iteratively and intentionally. Scope creep is an indication of disregard for requirements analysis, system design, and project management.

⁴² This term is used non-perjoratively and meant with the utmost respect for the relentless fashion with which Mr. McGarr pursued clarity and justice on this and other security/technology issues.

⁴³ Simon McGarr. "Primary Online Database: POD Now (mostly) Not Compulsory (for Now)." *Tuppenceworth.ie Blog*. August 31, 2015. <https://www.tuppenceworth.ie/blog/2015/08/31/primary-online-database-pod-now-mostly-not-compulsory-for-now/>. McGarr solicitors represent Digital Rights Ireland, an organisation “dedicated to defending Civil, Human and Legal rights in a digital age”, through legal challenges, working with legislators, and public activism. <https://www.digitalrights.ie/about/>

⁴⁴ Simon McGarr. "Hello and Welcome to My PSC Thread Entitled "I Told Ye So, so I Did."" *Twitter*. August 15, 2019. https://twitter.com/Tupp_Ed/status/1162142660360069121

⁴⁵ Elaine Edwards. "Woman's Pension Cut after She Refuses to Get Public Services Card." *The Irish Times*. August 22, 2017. <https://www.irishtimes.com/news/social-affairs/woman-s-pension-cut-after-she-refuses-to-get-public-services-card-1.3194216?mode=amp>

⁴⁶ The PPARS (personnel, payroll and related services) computer system was cancelled in 2005 by the Health Executive Service after ballooning costs and system inadequacies.

⁴⁷ I dedicated a chapter of my PhD thesis to this problem, see *Chapter 4 Organizational Issues* in: Margaret McGaley. “E-voting: An Immature Technology in a Critical Context”. *PhD thesis*, Department of Computer Science, National University of Ireland, Maynooth, 2008.

⁴⁸ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York, NY: PublicAffairs, 2019).

of the “darkening of the digital dream and its rapid mutation into a voracious and utterly novel commercial project.”⁴⁹

Zuboff cautions against “confusion between surveillance capitalism and the technologies it employs.”⁵⁰ We have taken on new risks with our new technologies—risks to the protections provided by our entitlement to privacy, to the sovereignty of our electorates, and to hard-won protections for workers—but it is not the technologies themselves that threaten us. It is the policies under which they are deployed, and the power structures we have allowed to be created around them.

I miss the Internet as it was in 1997. We told each other that “data wants to be free,” that the web was too wild a thing to be captured by commerce. We believed that we had discovered a new frontier that was so open and connected that it would change humanity for the better. We were naive to think that such a thing would develop on its own, unopposed, but perhaps if we are intentional, we can still make it happen.



⁴⁹ Ibid, 14

⁵⁰ Ibid, 21