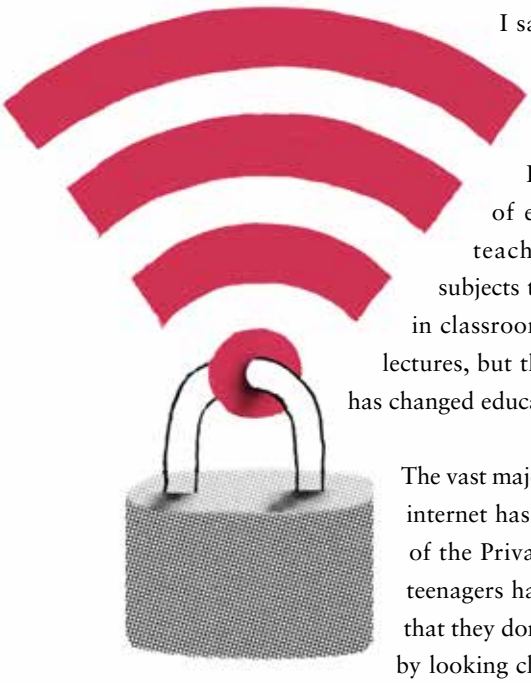
TO 2049 AND BEYOND

A FUTURE HISTORY OF THE INTERNET

ARTICLE BY
JENNIFER BAKER

Just as the advent of the internet has reshaped the world over the last 30 years, its evolution over the next will also define the society of the future. Digital geek Jennifer Baker tells the story of a Europe in 2049 that has harnessed and democratised the best of the internet, but that to get there had to experience the worst.

"2019 was the year people switched off Facebook." That's how I'm going to begin my lecture on the history of the Privacy Wars and the New Internet to my year threes.



I say my year threes, but in fact I've only met a dozen of the many thousands of 14-year-olds I teach every year. First rolled out four years ago, the European Remote Teaching Programme has been a huge success. Hundreds of experts and highly qualified professionals teaching students over the internet about the subjects that really matter. Trained facilitators are still in classrooms to help the kids get the best out of these lectures, but the general consensus is that remote teaching has changed education for the better.

The vast majority of my students take it for granted that the internet has always been a force for good, so the history of the Privacy Wars may come as a shock to them. But teenagers have not changed so much in the last 20 years that they don't understand the need for privacy. We'll start by looking closely at the Facebook shutdown that started in 2019, before covering the years leading up the Privacy Wars and then seeing how EU policy helped shape what was to come.

FIRST STEPS AND THE FACEBOOK SHUTDOWN: 2019-2028

To my 14-year-olds in 2049, the very idea of Facebook is baffling – the only online space where you could hang out and chat to people for free was owned by a company? Now, thanks to the InternetSpace4EU programme set up in 2028, a free, open space to meet and discuss online is maintained and moderated by independent authorities and supported through EU funds. When the space was first established 21 years ago now, its designers drew heavily on the work of digital rights campaigners, inspired by their embrace of the creative and democratic potential of online communication and their dual mistrust of private monopolies and unchecked state censorship.

More than 5 billion people were using the internet by 2020. It took nearly 10 years – from 2019 to 2028 – but eventually the voices speaking out for the internet's structure to be managed and regulated as part of our global public sphere were heard. In 2016, the United Nations Human Rights Council passed a resolution for the "promotion, protection, and enjoyment of human rights on the internet" which condemned any country that intentionally disrupted the internet access of its citizens.[1] The right to online access (the European Commission clarified in 2027 that this was an intrinsic part of the European Convention on Human Rights Article 10 on freedom of expression and Article 11 on the freedom of assembly and association) now goes even further, granting citizens the right to access the internet regardless of cost. Establishing unrestricted internet access set the EU apart from the rest of the world; it became a beacon for nations to follow. Without these two landmark movements, the online world would not now be as open as it is.

But back to the Facebook shutdown of 2019-2020. I will have to explain to my incredulous 14-year-olds how people back then were allowing companies to control their data. It's not that people were stupid, it's more that they didn't realise what was being done. No one knew how much data was actually worth and most people had never even heard of the enormous data brokers such as Acxiom and Oracle operating behind the scenes. The Cambridge Analytica scandal that broke in 2018 began to change all that. People started to switch off.

The General Data Protection Regulation (GDPR), introduced by the EU in 2018 to protect citizens' privacy, was to fundamentally alter the internet forever. Since the inception of the internet in the early 1990s, data had been gaining importance. By 2019, it was the

1 United Nations Human Rights Council (27 June 2016). *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/32/L.20. Available at <bit.ly/29jpSS4>.

main currency of the World Wide Web, used in advertising that kept many free sites alive. But the GDPR, and even more so the ePrivacy Regulation signed in 2021, began to restore the users' expectation of privacy. When it finally came into force in 2022, the regulation included a ban on 'cookie walls'. The whole notion seems outdated now, but at the time it massively changed the balance of power between users and companies.

THE HEAT OF THE PRIVACY WARS: 2025-2030

But as is often the way, things got worse before they got better. Throughout the late 2020s, privacy became a bargaining chip. Increasingly wealthy Europeans, Americans, and East Asians purchased services that were previously free of charge to avoid tracking and profiling. In Europe, business models shifted in line with the ePrivacy regulation, which favoured sites offering genuine services over those dependent on advertising.

In other parts of the world, tracking remained the norm. People could not afford to pay for services, and globally a two-tier society of the privacy 'haves' and 'have nots' emerged. Particularly in the US, those who had money paid for privacy while others went without. In large parts of the world, especially in the Global South, weak net neutrality led to the internet being nothing more than walled gardens run by tech corporations. People's understanding of the internet was limited to the four or five apps that came with their mobile phone package. Alarmed, the EU further strengthened its own net neutrality laws in 2029.

By the mid-2030s, the World Wide Web was effectively balkanised. Different world regions and countries sealed off their internet universes from others through a mix of blocking, decreasing interoperability, regulation, and physical infrastructure. Totalitarian regimes favoured the restricted Chinese model – heavily monitored with very little free flow of information. There was the two-tier American model driven by corporate avarice, and of course, there was the Dark Web.

The Chinese model and the Dark Web still exist to some degree. I don't like to encourage my year threes to think of the Dark Web as cool, so I tone it down. The Dark Web describes a section of websites that are on an internet-connected network, but that are encrypted so they cannot be found by traditional search engines or browsers. Essentially, they are non-indexed websites – like buildings that are not marked on a map. "So you can't find them unless someone tells you how to get there?" I can already hear them wonder. "That's kind of the point," I explain. But what of the American corporate model? "What happened to it?" my students ask.

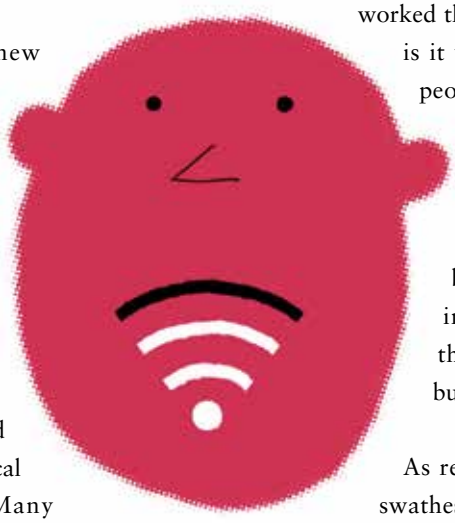
Throughout the 2020s there were calls by the European Parliament and various national authorities to break up Google and Facebook. It was feared that their mass of aggregated data allowed these corporates not just to track but also to manipulate people. The first outcry was over the 2018 Cambridge Analytica scandal, but it was felt all the more intensely following state-sponsored interference in the 2024 European Parliamentary elections. In parts of the world, the rule of law wavered between 2021 and 2026 as deep fakes and sophisticated disinformation undermined trust in legitimate governments. Elsewhere, technology was, as it still is in places, used to keep autocratic governments in power through surveillance. Internet shutdowns were particularly pervasive in central Africa.

As early as 2018, the EU had promised to tackle the question of data as an asset in mergers and competition cases. With the growth of machine learning, artificial intelligence, and what was back then called the Internet of Things (the increased interconnection of everyday objects via the internet), data was power. Businesses developed new models and found efficiencies through analysing massive data sets. As these were concentrated in the hands of a few corporations, policy-makers became worried. Companies had previously 'promised' not to merge datasets (as Facebook had done when it bought WhatsApp in 2014… before merging the datasets). Instead, laws were amended so that competition authorities could examine datasets when considering mergers.

That effort was stepped up in 2020 and data became one of the most important assets to assess in any merger, much to the chagrin of big American and Chinese corporates trying to snap up smaller firms. Some went even so far as to lay the blame for the recession in the mid-2030s at the door of these well-meaning "do-gooder" regulators who had undermined

dominant business models. Putting people before power made everyone poorer, critics claimed.

On the political front, new electoral laws spread throughout EU member states and overt political advertising became subject to strict conditions in almost all states by 2024. Even former EU countries that crashed out of the bloc over failure to respect the rule of law had adopted new rules on political campaigning by 2033. Many argue that in several countries those rules only serve to bolster the status quo, but we'll come back to that another day.



THE LONG RECESSION: 2030-2035

Although the internet changed substantially in the decade leading up to 2030, even in Europe old business models persisted. Many multinationals continued to try to skim as much data as possible from (increasingly savvy) users to sell on. But with the emergence of the two-tier privacy system and the ongoing Privacy Wars, those giving away their data were predominantly those who could not afford to do otherwise. And this is where we get to the real crux of the matter: advertising is only as valuable as the goods, products, and services being sold. Even my 14-year-olds worked this out pretty quickly: is it worth advertising to people who cannot even afford basic services? With no one spending, even the most manipulative of behavioural advertising firms discovered that their houses were built on sand.

As recession struck, large swathes of America fell into poverty, driving political upheaval and an even greater widening of the gap between rich and poor. China all but shut its doors. The Chinese money that had been pumped into buying foreign corporations slowed to a trickle. Europe, often seen as the slow-moving, dignified old woman of the internet, gradually took the lead.

Having become much less hooked on the data and advertising model, Europe's economy was not hardest hit when the recession came and was free to set its wheels in motion to slowly regain economic stability without worrying about big corporates collapsing. In simple terms, Europe had not grown as quickly as the US and had less to lose.

In other ways, the EU's approach to online governance had set it up for stability and recovery. A big push throughout the 2020s had led to digital services, such as eGovernment, single sign-on, eHealth, and cross-border single taxation being provided by governments to citizens in as efficient a way as possible across the EU. Reducing administrative costs in public services might not seem like a huge economic advantage, but when rolled out across an entire continent, the impact was impressive.

The growing sophisticated eGovernment network also demanded state-of-the-art cybersecurity. So much so that despite growing economic and political turmoil around the world throughout the 2030s, Europe became the place to be if you wanted to work on cutting-edge cybersecurity. The EU institutions invested heavily in relevant research. Even the constant demands for weakened encryption from national security authorities became less strident as the EU started to understand its competitive advantage.

A DIGITAL COMMONS EMERGES: 2035-2049

Of course, data had never just been about advertising. The significant advances in artificial intelligence could not have occurred without access to large data sets. However, before machine learning could be allowed to progress too far, there were many debates about its social, economic, and security impact. In 2018, global human rights organisations launched the Toronto Declaration, calling on leaders to address questions of discrimination resulting from the use of machine learning systems.

Over the following five years from 2019 to 2024, policy-makers worked with academics, businesses, and civil society to develop a Digital Data Donor Card. Much like an organ donor card, it allows holders to say for which purposes their data can be used. While many people were concerned about political advertising, most were happy to allow their data to be used for the good of society by ethical artificial intelligence, today widely seen as responsible for our longer life expectancy, cleaner cities, and excellent education system.

Some experts had predicted 'full connectivity' by as early as 2023. In reality it took a little longer and 'all human connectivity' was eventually reached in 2030. Nevertheless, there were still those who didn't quite trust the online world, and from 2035 a debate opened about the right to switch off. A sizeable minority decided they wanted nothing more to do with online life, preferring to pay in cash and meet in person. The EU issued guidelines for stating that, "as far as was reasonable", public authorities should provide an alternative offline method to interact with citizens. In practice, this means one small, usually quiet office in most large towns.

2038
Horizon 2060 project funds open internet space

2040
3DNet Everything Converter invented

2042
Discovery of the new electromagnetic spectrum

Instead the push was not for alternatives to online spaces, but for better online spaces. Surprisingly, it was not younger people who led the march for new ways to communicate and be social online. The internet as a commons was a movement led by people who remembered the offline spaces where people used to be able to talk – the local post office, the pub, the library, the streets. Creating these sorts of spaces online was only made possible by new platforms, whose continued development is being supported through funding from the EU's Horizon 2060 project, established in 2038.

Looking back from 2049, the years when the internet was monetised purely for corporate gain looks like an anomaly rather than the norm. As much as now, people back then valued freedom of expression and free speech, but perhaps did not understand the right to privacy in a public place as instinctively as my students today. Viewed from 30 years ago, the concept of 'privacy in public' is complicated. Partly because in 2019, online, all those public spaces were owned spaces.

In an offline, pre-internet era, everyone had the reasonable expectation of a certain anonymity, even in public space. As you walked down the street, you had the right not to be spied upon or followed. And yet by 2019, that is exactly what was happening to everyone who used the internet. It was the open-source community that got behind the internet as a commons idea and worked to create these safe yet public spaces where people could interact without handing over their data in exchange. Although part-funded by the EU, these spaces are protected by transparency and independence rules, last updated in 2045. No one owns these spaces and the organisation that runs them is depoliticised.

THE NEXT NET: 2049 ONWARDS

This all seems like ancient history and today material, not data, is the lifeblood of the internet. With the discovery in 2042 of an entirely new section of the electromagnetic spectrum, mobile connectivity is

expected to surpass anything our forebears could have imagined. But the 3DNet remains the biggest breakthrough of our times. The so-called Everything Converter is the internet for the 2049 generation.

Developed in Copenhagen, and making its semi-public breakthrough in 2040, the Everything Converter breaks down waste materials at molecular level and repurposes them for 3D printing. 100 per cent recyclability became possible. Early prototypes were too big and cumbersome for any house and many believed only large-scale use by commercial or public authorities would ever be viable. But, echoing the open-source cooperative movement that rebuilt internet space, communities clubbed together to use the Everything Converter at a local level and eventually created a device that could change everyday household waste into printable fibre.

Of course, this is of little use if you lack the design tools to tell your machine what you want to build. The big currency now is design. People share 'patterns' for products. The only thing standing in the way of people building whatever they want is the blueprint, not the material. Is this revolutionising society? Of course, and we don't fully understand what it might yet mean.

My students have a social conscience and, while they love playing with their 3D toys and trading the latest designs, they're aware that there are still those in the world who are less fortunate. This revolution should be for everyone, not just the chosen few. Looking back, the Privacy Wars and how the internet changed over the 2020s and 2030s should teach them this, if nothing else.

JENNIFER BAKER
has been a journalist in print, radio, and television for nearly 20 years. For the past eight years, she has specialised in EU policy in the technology sector.