1

"Privacy is dead – get over it!"

Silke Järvenpää
A provocative title this! And one that unfortunately I cannot lay claim to. Neither, it must be added, is the proposition to get over the death of privacy particularly new. The above, for instance, is a bastardised quotation from 1999, of a comment by Scott McNealy, CEO of Sun Microsystems. At that time, the company was a member of the Online Privacy Alliance. A consumer group had just criticized INTEL’s launch of a new chip that gave away identification information.¹

The dismissive remark stuck and has since been used by all and sundry, from Mark Zuckerberg to James Comey, then director of the FBI – who used it after the public was upset about what the Vault 7 WikiLeaks had disclosed.² The exposure informed about the CIA’s spying techniques in March 2017 and is considered to be the biggest leak of government surveillance since the revelations by whistle-blower Edward Snowden in 2013.

McNealy’s comment that became a meme is borne of the conviction that the idea of privacy is a ‘cultural thing’. As such, if we accept any of the contemporary definitions of culture (“a set of attitudes, values, beliefs, and behaviours shared by a group of people”), culture is dynamic.³ In other words: Would it not be natural that with change brought about by technological development in the digital age, value systems should follow suit? Why then would one cling to outdated ideas, but to show one’s resistance to progress?

¹ What Scott McNealy actually said when challenged, was: “You have zero privacy anyway. Get over it.” – The online magazine ‘Wired’ reported it on 26 January, 1999 (“Sun on Privacy: ‘Get over it’”).


³ For a contemporary definition of culture, see, e.g. D. Matsumoto, Culture and Psychology. Pacific Grove / CA 1996, p.16.
In fact, much of Silicon Valley (but also government agencies) have been keen to show that “privacy may be an anomaly”.\(^4\) Let me just cite another examples here, apart from Vint Cerf. Technology journalist Greg Ferenstein provides us with a very American overview over “World History”.\(^5\) He points to the absence of private spaces in tribal communities around the world, in ancient Greece, Rome and the Middle Ages, and well into the 19th century, before Supreme Court Justice Louis Brandeis formulated, for the first time in US history, a right to privacy.\(^6\)

At first sight, Ferenstein’s argument appears temptingly plausible: It is true that poor people’s houses accommodated entire families, that sexual intercourse, for instance, took place before a number of witnesses. It is also true that when King Louis XIV awoke, it was a public event – at least for those admitted to his levée. From their historical examples Ferenstein (and others) deduce that humans have obviously always valued convenience, security, and wealth over privacy, and that the whole debate on privacy is luxury at best and decadence at worst.

Apart from the fact that those evangelists of the Valley see tribal cultures as comparable to Westerners in the stone age (a slightly problematic understanding of history), they do not engage in sound research to begin with.

Those who do, like Law professor Joseph Cannataci and anthropologist Irwin Altman among them, arrive at different results: The idea of privacy, they find, is valued highly in almost all cultures around the world, and was


in almost all historical ages. The definition of privacy may differ from region to region and from age to age. But as an idea of value and importance it is universal and part of human nature rather than culture.\footnote{Cf. Joseph Cannataci, The Individual and Privacy, vol. I. Routledge, 2016.}

The \textit{20th} and early \textit{21st} centuries, at least, are dominated by resistance to the notion that the erosion of privacy should be become a non-issue. After Vault 7, the print edition of the ‘Süddeutsche Zeitung’ chose a cover that featured the eye of a web camera attached to but disproportionately upstaging a television set. The headline read: “Ausgeguckt. Was Geheimdienste anstellen, um jedes Wohnzimmer ausspionieren zu können”.\footnote{Süddeutsche Zeitung, 11/12 March, 2017. Cover Credit: AP, Allessandra Schellnegger et. al.} But in 1997 ‘\textit{TIME Magazine}’ had already offered a cover story focusing on “The Death of Privacy” and drove home the message by the image of a non-descript individual, shady in every respect, who peeps through a stylized keyhole. And as early as 1970, ‘\textit{Newsweek}’ devoted an edition to the self-same topic with a picture that is almost endearing in its pre-digital fears (here anthropomorphic computers fed with punch cards, and other old-fashioned wire-tapping devices dwarf a frightened John and Jane Doe).\footnote{\textit{TIME Magazine}, 25 August, 1997, cover credit: Matt Mahurin; \textit{Newsweek}, 27 July, 1970, cover credit: John Huehner-Garth.} – Despite the cultural differences that are to be expected across decades and continents, the three cover stories, including their visuals, share common features, the most relevant being the link between the death of privacy and large-scale surveillance measures.

This is where advocates who try to convince us that privacy is an anomaly try to pull the wool over our eyes. Most people do not mind a casual intrusion to privacy as much as a systematic one; they do not mind spectators as much as monitors. When the loss or death of privacy is lamented nowadays, complaints are about surveillance, in other words to the “focused,
systematic and routine attention to personal details with the purpose of influence, management, protection or direction”.\(^\text{10}\)

There is good reason to see contemporary surveillance critically, and to dismiss arguments along the lines of “If you have nothing to hide, you’ve got nothing to worry about”. The past is again elucidating and has shaped critical surveillance studies. It was the 18\(^{\text{th}}\) century, when the debate about privacy was born. A number of Enlightenment philosophers were no longer convinced that God’s all-seeing eye impressed people very much in their lives and decision making. In fact, so much management, direction and influencing was taking place behind closed doors. It was the privileged who were privy to information; they ruled in relative privacy.

To Utilitarians, whose ideal society was one which would bring the greatest benefit to the greatest number of people, privacy became a dirty word.\(^\text{11}\) Jeremy Bentham, a judge and philosopher, insisted that an end to privacy would be the solution to most ills in society. Total transparency turns into a moral value: “Without publicity, no good is permanent; under the auspices of publicity, no evil can continue”, he claimed.\(^\text{12}\) In order to reform society, all institutions were to be built with cost-efficiency and total transparency in mind. Bentham started by proposing the design of a prison whose very architecture would better its inmates. Its name: the Panopticon; its method: total loss of privacy; its economy: random surveillance by a few watchmen. To scholars of Surveillance Studies, the principle of the Panopticon still serves as a model of contemporary cultures of surveillance, and it will soon become clear why.


Bentham did not live to see his own draft realised, but in the 19th and 20th centuries, Panopticons were actually built; the most famous examples being the Presidio Modelo in Cuba and Stateville Prison in Illinois, USA. A Panoptic prison has a watchtower in the centre; the cells are arranged around it. The inmates cannot communicate with each other; they can see the tower but not the guard in the tower. The guard is not capable of monitoring each prisoner at every given moment, but the prisoner knows he may be watched at any time.

The psychological effect of the Panopticon is a disciplinary one. The prisoner is subjected to the power of the watchtower, totally and around the clock. Anticipating the guard’s gaze, he checks and self-censors his behaviour.

In the 20th century, French philosopher Michel Foucault saw in the Panopticon the construct that permeated contemporary society everywhere – where power was exercised through bringing visibility and instilling discipline instead of exacting revenge (by torturing transgressors and killing them in public spectacles as a warning to all that were not and could not be monitored). Foucault also saw all modern institutions based on the Panoptic principle: schools, factories, hospitals. In his eyes, it had become an ideology which he called Panopticism. And this was well before the so-called digital age.

“The Panopticon is a marvellous machine which, whatever use one may wish to put it to, produces homogeneous effects of power. A real submission is born mechanically from a fictitious relation. So it is not necessary to use force to constrain the convict to good behaviour, the madman to calm, the worker to work, the schoolboy to application, the patient to the observation of the regulations.”


The idea that what we do may not be in privacy, will lead to self-monitoring, to self-censorship. Ultimately, we will internalise the Panopticon.

Proponents of surveillance nowadays (surveillance which is supported by almost unlimited technological means for the purpose) often argue along Bentham’s line but frame the debate in a positive way. If surveillance helps to maintain order in society, that order will create safety; and this will benefit the majority. Firstly, we see a classic argument by state authorities: Particularly in Western countries, the discourse of privacy is played out against the discourse of security (who would not want most people to be safe?) Secondly, we tend to observe authoritarian fear mongers following the same strategy, with their most drastic slogan along the lines of “Privacy is for pedos” (i.e. paedophiles).\textsuperscript{15} – Accordingly, the mere wish for privacy is a reason to raise suspicion.

Apart from the (self-)disciplining function of the Panopticon, Foucault and Bentham uncovered two more. The Panopticon also has the potential to classify and to sort; it is likened to a menagerie, or in other words: a zoo. Moreover, it serves the purpose of a laboratory, or in Foucault’s words: a “machine to alter behaviour, to train or correct individuals”.\textsuperscript{16} Ultimately the watched will not only obey the law but conform to the desired norms.

If this is the Panopticon’s potential before the digital age, then what we are dealing with nowadays, is practically a Panopticon on steroids. It is not difficult to see why the combination of the Idea (of Panopticism) and technological progress proves to be particularly toxic and may indeed usher in the death of privacy.


\textsuperscript{16} Foucault (see footnote 14), p. 203.
What made sorting and classifying as well as social engineering a demanding task in the past was the resources needed to collect the data, to analyse them and to turn data into usable information. Networks tended to be wide-meshed. There was a natural limit to storage space, and even semi-automatic measures taken after sorting, lacked consistency and completeness. Often, there was no access to data across borders (such as card catalogues); so Panopticons, though they were in place, existed as contained systems.

Nowadays, storage space no longer is an issue. George Brock who traces data protection laws up to ‘The Right to be Forgotten’ states that storage “is expected to grow to 44 zettabytes in 2020”. This means that, technically, state authorities, agencies and corporations are capable of collecting any amount of an individual’s personal data and keep it forever. When databases are joined, each adds missing parts to a puzzle.

Sorting, too, poses no problem. In fact, sorting algorithms have become so sophisticated that the confluence of data and its interpretation make it possible to provide a well-neigh complete profile of an individual. The knowledge that databases may have about us is probably more complete than what a spouse, one’s parents or best friends, or what even a psychotherapist may have after many years of being privy to the life of that individual.

Why that should be so threatening may not be immediately apparent. Most human beings, when they go online, define themselves as social creatures and not least as consumers. They chat, make appointments, buy online, self-monitor their health status, and do not mind the collection of their data much.

They appreciate advertisement that targets their tastes. It is convenient, and convenience is a strong driver also when it comes to accepting the

terms and conditions of online banking, holiday booking systems, and other e-commerce activities. To many customers the exchange of data for services seems like a win-win situation.

What most do not realise, however, is the fact that those activities become their internet identity - an identity they have only limited control over. Users may be able to decide what they post on Facebook or WhatsApp. However, consumer habits, movements, contacts, writing style, vital scores (transmitted via activity tracker, as for instance fitness bracelets) speak their own language. With the disclosure of bio-data users will be better known to the Panopticon than to themselves.

Or, as social philosopher Zygmunt Bauman noted, “[…] the information that proxies for the person, and in the legal sense is made up of ‘personal data’ only in the sense that it originated with a person’s body and may affect their life chances and choices. The piecemeal data double tends to be trusted more than the person, who prefers to tell their own tale.”18 With the end of privacy it becomes harder and harder to manage one’s own identity and to plan social interaction with others – two functions that privacy fulfils.19 Those that do manage one’s identity are the ‘watchmen’ who by default assess, influence and direct based on their value systems and norms. Add to that algorithms which do the groundwork, and consequences are, at times, disastrous.

One particularly Kafkaesque example is the “terrorist watchlist”. Officially, there is no such list. When ‘The Intercept’ published leaked information on it, however, the US administration no longer denied its existence. It turned out that a person’s own activities are not the only way to end up on the list. If you and an Islamist’s path cross more than once, maybe in front

---


of the same ATM – and Geo-tracking shows where you have been – this may make you a suspect; if your network of followers on Facebook contains known suspects, you may be declared guilty by association.

As Bauman wrote, your data double tends to be trusted more than you. Embedded in the security discourse, we are seeing immense faith in computing algorithms. Once ‘the machine’ suggests to a small committee of government agents that your data double shares with terrorists a certain number of markers and that therefore you should be added to the list, the human agents will follow the suggestion of ‘the machine’. The fallout of such decisions may ruin your real-life existence:

“Once the U.S. government secretly labels you a terrorist or terrorist suspect, other institutions tend to treat you as one. It can become difficult to get a job (or simply to stay out of jail). It can become burdensome – or impossible – to travel. And routine encounters with law enforcement can turn into ordeals.”²⁰

It is interesting that with the digitalisation of the War on Terror, law enforcement has left the rule of law. The watchlist is pre-emptively punitive. It highlights what is ‘not normal’ and what may lead to disorder. For society at large, mass surveillance with the aim of creating profiles for security reasons may therefore mean the end of a creative and dynamic culture. If people are aware that a system is in place which classifies, corrects, and re-trains before unusual things, including unusual ideas, can mature, the Panoptic effect of anticipatory self-censorship kicks into gear. The exchange of unorthodox ideas, ultimately even thinking those ideas becomes something better to stay away from. It is no wonder then that critics of surveillance have seen an Orwellian dimension to this: Big Data and digital profiling also are about ‘thought-policing’.

However, Big Government is not the only actor that invades an individual’s privacy in order to manage and direct in dubious ways. Big Business, too, is using personal data to sort – and ultimately to exclude entire communities. In her book ‘Weapons of Math Destruction’, mathematician Cathy McNeil convincingly shows how ‘Big Data increases inequality and threatens democracy’ (as the subtitle reads). The cases from private enterprise are compelling:

“With ever more information available, including the data from our genomes, the patterns of our sleep, exercise, and diet, and the proficiency of our driving – insurers will increasingly calculate the risk of the individual and free themselves from the generality of the larger pool. […] Insurers are using data to divide us into smaller tribes, to offer us different products and services at varying prices. Some might call this customized service. The trouble is, it is not individual. The models place us into groups we cannot see, whose behaviour seems to resemble ours.”

While Bauman’s idea of the digital self as a proxy for the person resonates here, McNeil focuses more on the joint liability the individual is subjected to through algorithmic sorting. With Big Data (some of it bought, some of it extorted, but much of it served on a silver platter by consumers and clients) insurers for instance, adapt and fine-tune their policies. With the growing complexity and capacity of algorithms, insurers tend to believe in the objectivity and infallibility of their calculations. After all, assessment is left to the machine. But as McNeil points out, the model was built by humans.

To return to Foucault: Collecting, sorting, profiling, and managing – all of this reflects the power structure of a Panoptic culture. Sorting and profiling will be informed by the value system of the watchers. That value system will partly be based on the norms and values within a certain region at a certain point in time, and not least reflect its prejudices. Presently, the

African-American community tends to be seen by corporate and political America almost like a monolithic bloc: financially weak and crime-ridden. In Germany, clients of Turkish descent might be penalised for excesses in their community, because the algorithm identifies them as members of a high-risk group. But while culture is dynamic and biases may slowly change, “automated systems stay stuck in time until engineers dive in to change them.”

Another part of the bias behind a corporate algorithm will be due to the simple fact that businesses are in it to make and maximize profit. If the predictions of an algorithm, however faulty they may be, promise that the exclusion of entire communities will lead to more profit, Big Data will indeed be exploited for that.

It should have become clear by now that loss of privacy in the world of Big Data means loss of control over one’s own identity management. The information an algorithm creates based on a seemingly sound pool of data will predict how you act and will act in the future. That in turn will decide over treatment you receive, including the opportunities you will be given in life.

So the death of privacy is something that should, in the interest of both the individual and the group, be at least delayed. Gary T. Marx, sociologist and scholar of surveillance, offered a typology of resistance in 2003. – Meanwhile technology and the ubiquity of surveillance have evolved and some advice has become obsolete in the face of further erosion of privacy. However, what both scholars and activists agree on is that there is benefit in challenging the status quo. Such activities have effected change, in the form of legal victories, or awareness of surveillance measures after leaks to the public.

22 Ibid., p. 203-204.

But apart from very concrete steps that one can take – from encrypting mails to whistleblowing to going to court – working towards change must also include attempts at breaking present discourse hegemony. What the debate needs is a struggle for different interpretations of reality. So far there has been a tendency to juxtapose surveillance as a subtopic of the security discourse (working for the benefit of the community) with privacy (allegedly only of individual interest and therefore subordinate to group interests). A different interpretation could reframe the debate as a question of surveillance and human rights. It goes without saying that language is important in changing perception of reality.²⁴

²⁴ From dataveillance to überveillance and the realpolitik of the transparent society: the second workshop on the social implications of national security, ed. by Katina Michael and M. G. Michael Wollongong 2007, p. 71-82.