Check for updates

Standard Article

CCJ

Criminology & Criminal Justice
1–17
© The Author(s) 2023

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/17488958231184695
journals.sagepub.com/home/crj
Sage

Exiting the captaverse: Digital resistance and its limits pre and post the Covid-19 pandemic

Janos Mark Szakolczai
University of Glasgow, UK

Abstract

The term 'data', ubiquitous in the Digital Age, etymologically refers to a piece of information 'given' (datum). In this article, I argue that the term 'capta' would be more accurate, since information is often taken from us. Capturing information replicates normative elements of abuse, surveillance, control and harm becoming central and problematic within the emergence of the 'onlife'. I illustrate my argument via an ethnomethodological consideration of my attempt to resist the unwilling capture of personal information. Since 2016, I have engaged in what I call an 'offlife' existence, phasing out all devices and platforms that covertly capture personal data. However, my experiment has proven problematic, impractical and has even been perceived as being anti-social, especially in light of the Covid-19 pandemic. In the conclusion of this article, I consider the problematics of engaging in some form of resistance to data collection.

Keywords

Big Brother, bigdata, capta, Covid-19, covidiots, cybercrime, Deleuze, desistance, digital harm, e-health, FOMO, obfuscation, onlife, panopticon, surveillance

Data-as-given

The word 'Data' originates from Latin: it is a datum; something given. Thus, a piece of something, namely, a piece of information, 'handed' consensually out. The use of 'data' is a recurring problem of our Internet engagement. 'Data' are taken and kept from users – analysed and monitored, on a regular and spiralling and "liquid" basis (Bauman and Lyon, 2013). This metrical gathering, storing and recording (Beer, 2016) of users' digital activity, including clicks, swipes, likes, purchases, movements, behaviours and interests

Corresponding author:
Janos Mark Szakolczai, The Scottish Centre for Crime & Justice Research, University of Glasgow, Glasgow, G12 8LR, UK.
Email: Janosmark.szakolczai@glasgow.ac.uk

(Christl and Spiekermann, 2016; Lyon, 2018), and generalised use of biometrics (Pugliese, 2012), occurs in a ubiquitous and unsanctioned manner (Nissenbaum, 2015). This leads to the extreme offering of an open view into our 'soul', in the poignant words of G.T. Marx (2016), especially recalling a 'totality' of elements of harm, surveillance, monitoring and control (Giglioli, 2019). The currency of the 'cyberage' has been connected within the 'big picture' of harm (Redden et al., 2020), intensifying among others, elements of cyberstalking, flashing (McGlynn and Johnson, 2021), aggression (Marganski and Melander, 2018), doxing, trolling (Lavorgna, 2021) and toxic social surveillance (Trottier, 2019). This is particularly significant if we acknowledge the rhizomatic means of control (Deleuze, 1992), and the surveillance assemblage it constitutes (Haggerty and Ericson, 2000), leading to the quintessential 'dragnet' environment (Angwin, 2014) academics and researchers have been investigating for the last decades. From the perspective of digital harms (Wood, 2022), cyber harms have become an encompassing reality (Lavorgna, 2021), limiting any resistance, and taking over what Luciano Floridi (2015) considered an 'onlife' engagement (online + life). The theoretical bases of this article are the considerations offered about aspects of control in the digital age by Philip E. Agre and Gilles Deleuze. In particular, Agre (1994) saw the elements of 'Captivating Surveillance' as a growing aspect of our digital engagement and relation with technology. Deleuze (1992) perceived the novel and encompassing elements of control that evolved from Foucault's (2008 (1978)) disciplining societies. I explore the ideas of Deleuze and Agre not only due to their theoretical relevance but (metaphorically) also as real-life responses and dissent to the englobing scenario they saw before them. Deleuze incidentally opted out of his dystopic Society of Control ending his life in 1995. Agre chose to go 'off the grid', and literally disappeared in 2009 (Pescovitz, 2009). My article discusses my ethnographical attempt to engage with an alternative, from 2016 through (most of) the Covid-19 pandemic. Having grown up in the digital revolutions of the late 2000s, I literally dived into all major social networks and interacted enthusiastically with all the latest mobile technology & smart media novelties. Though curious, my involvement was never without criticism, and over time my concerns grew over the potential, the manoeuvres and the implications these tools have on users. My scholarly objective was to allow an alternative sense of 'agency', as opposed to the fatalism of harmful data collection dynamics. Ultimately, I came to explore the idea of something not quite right in the implications of 'handing-out' our 'datum', and what, other than privacy concerns, is the harm involved.

The first step to do so was seeking a so-called 'offlife' engagement as to resist the rhizomatic formation of abusive data collection (Haggerty and Ericson, 2000). This involved specifically a social media suicide, self-limited Internet involvement and full-scale disengagement from smart devices. My objective was not simply to produce research data, but to become engaged in a novel, experimental hybrid ethnomethodological practice (Przybylski, 2020) that would be less problematic for me as a person and a user of the onlife. This aspect is central and significant today more than ever, in light of the setting of new scenarios for further data collection within the metaverse (Beer, 2022), and the means implied for the gestation of the Covid-19 pandemic. In both instances, potential harm appears underplayed. That 'privacy is dead' is a recurring mantra that has been recalled to us repeatedly, among others by Zuckerberg, who underlined decades ago

how privacy is no longer a social norm (Johnson, 2010). Though data collection is still to date perceived as controversial and problematic, at least from a privacy standpoint, its resistance is just as well quite limited and ignored (Brunton and Nissenbaum, 2015). Refusing the capturing of information becomes not simply a privacy issue (Lavorgna, 2021), but a question of resistance (see Ferrell, 2022), dissent (Selmini and Chiaramonte, 2022) and even, more specifically, a quest into modelling a subjectivity resistant to capta.[1] In this context, the connection of data and harm, including the cybercriminal and toxic elements of our constantly connected devices, becomes a focal element of our onlife experience. In contrast, my experimental offlife ecology proposes a perhaps utopian environment where users are more in control of their information and their data. The requirement is for our data – even when published voluntarily – to free itself from a *capta* establishment that perpetuates the conditions of having something taken and used covertly. Such an approach appears central in creating awareness and at the same time a guideline for resistance to avoid automatic flagging of those who are not integrated and limit the control of the biopolitical apparatus (Agamben, 2009), or, to put it simply, to permit some sort of alternative that does not imply some repercussion or make one look like a criminal (Vertesi, 2015).

Captaveillance

Digital data are trivially understood as the exchange we offer, almost reciprocally, for 'free navigation'. This gratuity is meaningless in a neoliberal milieu, being rather the compromise of a 'no-free-gift' (Douglas, 1950 (1990)) condition we have become accustomed to within our society. When users divulge and 'give away' their information, it appears as something 'out there for [anyone] to use' (Marx, 1998: 178): the idea of consent or choice within the online realm is 'disingenuous to the extreme' (Marx, 1998: 178). While we are offered consent forms when navigating the web, at least according to various Western regulations, what really takes place in the background of our digital existence is out of our reach or knowledge. Such argument is led forward by Byoung Chul-Hal in describing an aperspectival panopticon system, underlining its 'omnipotence of the despotic gaze . . . of everyone from everywhere, which anyone can perform' (Han, 2012: 45). As shown by yet another significant Facebook/Meta leak, data collection becomes not only as replete and boundless as ever but also impossible to keep track of (Biddle, 2022).

This falls short of Deleuze's conceptualisation of a 'surveillance assemblage' (Haggerty and Ericson, 2000), a prison-like yet discrete system where we are granted access to places and spaces only by constantly showing some electronic identification. 'Individuals have become "dividuals" and masses, samples, data, markets, or "banks"' (Deleuze, 1992: 5); non-abidance only leads to further marginalisation and exclusion. Internet critic Geert Lovink (2019) and scholars like David Lyon (2018, 2022), noticed how the devices we carry perpetually define us, sort us and enlist us, with potentially demeaning means. For Deleuze, who took forward Foucault's theories on the centrality of discipline within the notion of blind surveillance, the Societies of Control are mixed within an automatised system – an assemblage where surveillance grows into a truly

rhizomatic apparatus, conceived as operating 'by variation, expansion, conquest, capture, offshoots' (Deleuze and Guattari, 1987: 21).

Such taking rather than receiving was a central concern of Philip Agre already 1994, when discussing the nature and problematics of 'Captivating Surveillance'. The action of 'capturing' is for Agre an 'upgrade' to the Big Brother–like surveillance milieu. In detail, 'The capture model, like the surveillance model, is a metaphor system and not a literal description' (Agre, 1994: 107). The question of tracking in Agre's (1994) work is connected to automatism and Taylorism, addressing the twin imperatives of efficiency and control in the same fashion: 'by legislating the precise sequence of actions in advance' (Agre, 1994: 117).

Especially since the onlife engagement (Floridi, 2015), data are not simply a piece of information; it is the unity 'used to provide some sort of measure of the world' (Beer, 2016: 3). Data are the oil that lubricates the engagement, the advertisement, the tailoring and the functioning of the digital experience. These pieces of information are taken and kept from users – analysed, gathered and stored, on a regular and spiralling basis (Pasquale, 2015). The word 'data' is indeed perhaps too kind, if not simply misleading, because it gives a different light on what takes place, how and why. I suggest that the word 'datum' be changed to 'capta' in situations where harmful and secretive collection is taking place. This will better convey the idea of something being taken, rather than simply given.[2] These considerations over *data* and *capta* recur in other disciplines, such as archaeological research (Chippindale, 2000) and social sciences (Lanigan, 1994). The discussion is surprisingly stale and has a somewhat anachronistic reckoning. Capta appears as such not only the currency, but the coercive power of the systems built around us. It is a surveillance that takes all; it is purposeless if not to capture, that is, featuring a captaveillance dynamic. Capturing, as we will now discuss in detail, becomes a truly 'agnostic' (Lanigan, 1994: 116), and thus limitless stance. It shapes lifestyles and becomes central in the metrical form of power: 'the means by which our lives are captured, but in which that information is protected by commercial interests' (Beer, 2016: 108).

Captivating devices

Capturing information is a replete and recurring scenario. It takes place both in passive and in active terms. *Passive* captaveillance is evident with devices such as smartphones. Smartphones offer the perfect device and medium for this 'captivating' condition. It induces and partly seduces the user, thanks to the design of its features, inducing a specific 'data-producing' life. As noted by Giglioli (2019), this form of 'indirect' surveillance involves us, without ever actually seeming to 'touch' us. The smart tools are designed to produce and store pieces of information in what Siva Vaidhyanathan (2012) noted as a 'cryptopticon', drawing towards the 'cryptic, hidden, scrambled and mysterious' (Vaidhyanathan, 2018: 67) monitoring reality, where 'one can never be sure who is watching who and for what purpose' (Vaidhyanathan, 2018: 67). A smartphone, for example, is constantly in the user's pocket, functioning both when capturing signal or whether in 'aeroplane mode': it collects all sorts of information about users' whereabouts and usage with the use of sensors (GPS, barometers, altimeters) and usage-monitoring

(screen time, clicks, interests, communication) offers trivial functions for surveillance and monitoring, containing our most private information (including eHealth, more later). The design of our devices thus is only increasingly replicating the black-box creeping functions described by Frank Pasquale (2015), along with the crypto-elements of control and monitoring of everyone and everything (Herrero et al., 2021). The smartphone replicates the capturing of information, and does so endlessly, with new and new systems and upgrades. It becomes an agnostic scenario that users struggle to conceive, comprehend and limit – a point that is rendered even more clear with Dave Beer's consideration of algorithms forming a new social power that controls and monitors our web content (Beer, 2017).

From an *active* perspective, captaveillance involves users in 'taking' pictures, filming and audio recording; the 'capturing' of what is around is done with evident nonchalance, regular conduct that anyone with a smartphone can trivially, almost unconsciously engage with – showing very limited and blasé concern towards privacy violations (Giglioli, 2019). As Vaidhyanathan (2012) had noted already a decade ago, none of this was possible without smartphones. Nowadays, in the aftermath of the Covid-19 pandemic, we are more than ever limited within our connected yet detached compound.

From a criminological perspective, any Internet-connected device, especially due to its 'smart' functions, allows an active endless replication of all the elements of cyber harm: from stalking through doxing to doing surveillance – providing instances of capta collection. Cyber criminality has become an accepted if not trivial form of crime and criminality (Yar, 2005). What is permitted, and to what we have 'given' permission, loses its grasp in virtual scenarios. Cyberstalking as a form of captaveillance is significant, as an 'invasive form of partner monitoring' (Marcum et al., 2017: 375) can take place in apparent 'friendly' social environments, particularly aided by social networking platforms that become per se social surveillance websites (Tokunaga, 2011). Such episodes take place on university campuses (Marcum et al., 2017) as well as within internal communications of co-workers (Lowry et al., 2016). It takes place globally and in an all-aged (Horst, 2020) and pluri-gendered (Winkelman et al., 2015) reality. Stalking and bullying are particularly connected in this scenario, due to the insistence of offences (Forssell, 2016; Lavorgna, 2014; Shariff, 2014). Such dynamics show evidence of 'more psychosocial and emotional damage than traditional offline physical bullying because of the increased volume, scale, scope, and number of witnesses' (Gillespie, 2009, cited in Lowry et al., 2016: 963).

Going 'offlife'

By the mid-2010s, I contemplated how to detach myself, from the abovementioned harmful dynamics, without paying the price of a secluded life: a user of the onlife existence but at the same time an *offlife* participant. This was important for me both as a citizen and as a social scientist. I conceived the 'offlife' as a way of integrating Floridi's (2015) neologism 'onlife'. To be 'offlife' for me did not simply mean going 'offline', or 'off-the-grid' (Angwin, 2014). Instead, it consisted in systematically limiting the number of online sources, platforms and devices – in the likes of the notorious experiments by Vertesi (2015) who attempted to reduce the online visibility of her pregnancy. However,

I did not wish to disappear, if at all possible (Haggerty and Ericson, 2000: 619), nor strenuously confuse or mislead governments and corporations, but rather limit my 'capta' while engaging in a healthy social, cultural, intellectual and productive life. As the onlife existence involving smartphones, social media, networks, online maps, interactive apps, tracking devices, and freemium games surround us every day in a regular and complementary fashion, even a simple glimpse of the surroundings proved a significant source of study.

Building up from cultural criminology, my approach was much in tune with the ethnomethodological methods (Garfinkel, 1967), trying to identify the 'everyday life world' of onlife users and conceptualise 'drift' methods of engaging with their experiences (Ferrell, 2018). I offer a reflexive sociological and criminological consideration of the harms involved in captaveillance, faithful to 'the myriad forms of resistance and the repressive nature of acquiescence' (Ferrell et al., 2008: 205). All related considerations have rested solely on my lived experience – which becomes a central disengaged offlife element 'within' the onlife environment.

The initial difficulty involved in 'not-playing-by-the-rules' became evident when choosing the strictest-possible privacy-focused options on my browser. The result is one of not being allowed a proper navigation experience: access was limited or practically impossible on most websites. This, it seems, recalls the conditions as suggested by Deleuze (1992): Without the proper 'conduct' and acceptance of the 'rules' and conditions offered by the platforms, access is not granted.

To continue navigating freely, I instead followed the lead of obfuscating methods (Brunton and Nissenbaum, 2015). The approach of these scholars and computer engineers is a particularly helpful attempt to scramble users' data both online and offline. Using VPN software, privacy-friendly search tools, multi-layer encryption browsers and disposable emails helped to significantly reduce my clickstream, metadata and logs, thus avoiding or at least reducing to a minimum the 'very specific and personal narrative' (Brunton and Nissenbaum, 2015: 54). Such tools could have been well integrated with other platforms such as Duck Duck Go browsers, or even more efficiently (though somewhat lagging the browsing experience) via Tor and Dark Web that allow strict minimisation of captaveillance technologies. Also, I installed specific 'add-on' extensions on my everyday Internet navigation browsers, limiting tracking, disagreeing automatically to cookie collection and scrambling my very 'data', confusing it with non-pertinent information.[3]

However, obfuscating solutions and platform extensions do not limit the practice of captaveillance. Not that they fail in doing so, rather they are designed differently. Also, there is no evidence whether the corporation cannot very well, and precisely, recognise what content is 'bot' produced, and what is still perfectly identifiable and targeted to the ad personam user.[4] Moreover, many of the very add-ons and alternative browsers rendered navigation limited, on some websites impossible.

It became clear that if I cannot access social media and most websites on my terms, it made rather more sense to do without them altogether. I thus eventually decided to take a more 'radical' stance, the effects of which I will now illustrate seeking to avoid the occurrence of capta with the aid of four onlife contexts. I began by deleting all my social

media accounts, limiting myself to the use of smart devices, engaging only with analogical audio-video devices and generally reducing my digital footprint.

Social media

Indeed, as the limitation set by these self-imposed 'terms and conditions' made all navigation to prime social media services impossible, I decided in June 2016 to opt out and delete all my social media accounts.

Initial reactions to my disengagement led, to say the very least, to annoyance among my peers and the suggestion that I was 'missing out'. As the highlights of Cambridge Analytica in 2015 and so-called Datagate conditions had been recently brought to global attention, the 'disconnect' option appeared as a political stance. Years into my missing out on the 'social media' experience, my position was even more emphasised by the popularisation of documentaries such as The Social Dilemma (2020).[5]

Smart devices

The progressive disconnection that I embarked on was systematic but phased. After quitting all social media (Facebook, Instagram, Whatsapp), since 2018 I began to engage with my smartphone only as a sim-free tablet and used a GSM-only device to make calls.

My so-called 'feature-phone' lacked sensors – that normally in smartphones passively capture and calculate all sorts of metrics (altitude, barometers, GPS, accelerometer, pedometer, etc.), and was generally tougher built than normal devices.[6] The plastic has heavier, and the screen is significantly less fragile. Internet navigation feature was exceptionally limited, yet somewhat functional. It could not offer any playback option, nor download any picture or file. When accessing email via the mini browser, I had to insert my email and password every single time, confirming that there appeared to be no cache or cookies. The navigation did not know my location, and I never fully grasped what my IP address was. In this odd grey area, I felt vaguely protected and anonymous. My device never featured any advertisement or requested Cookie consent. I expected the browser to simply accept cookies as default, but I am not sure whether this was the case.

E-commerce and entertainment

Following the purpose of my offlife approach, I decided still in 2018 to unsubscribe from all those that I considered capta-gathering online services, including streaming providers of video/film and music media. Instead, I opted towards 'things' that offered per se a service that had no hidden, monitoring potential – similar to the more recent considerations of Han (2022) and his 'non-things'. I began investing in hard-copy material (CD and DVD) or hard-drive-shared digital material that would allow me to enjoy music limiting the productions of capta (via clicks, algorithms, likes and suggestions). I would read a wide range of printed newspapers from libraries to receive updates not only on the 'latest' news, but also read about weather forecasts, shows and events. I also attempted to consult dedicated dictionaries to clarify meanings and translations, rather than websites. The same applied to other kinds of guides; I tried to reduce to the bare minimum

my access to Wikipedia and other websites. My online purchases and transactions, given my disdain for use of data and working conditions of the gig economy and e-commerce providers, were reduced with great satisfaction to quasi-zero.

Digital footprints

Navigation and directions without a GPS service were one of the most controversial features, meeting with the greatest resistance from friends and peers. In discussing directions, I oftentimes ended up seeking locations on somebody else's map provider. Many peers sensed this as a 'parasitic' behaviour on my behalf: without my 'capta' of other users' data, I could not find my whereabouts. I 'compromised' my commuting by using an offline portable Navigation device while driving, to which I manually updated the map via SD card. However, when on foot I would use an offline map app strictly disabling GPS.

Through these practices and recognitions, a slow but evident 'skimming' of my screen time was palpable. Through my capta disengagement, I came to feel that not only my data but also my attention was less 'captured', and thus stolen from me. To date, mixed arguments have been forwarded on the actual validity of digital detox programmes (Ellis, 2019; Ghita and Thorén, 2021) – a practice promoted both in mindfulness programmes and by academics. I did, however, by limiting card transactions, online banking, delivery services, and felt I was slowly regaining my lost-to-'click-bait' identity, formed by my stolen data (Zuboff, 2019). Such a process felt particularly liberating in regard to the typical 'echo chamber' information control and other 'dark patterns' in UX techniques, whereas users are subtly and covertly 'tricked' into 'opting in' to services rather than 'out' (Fard, 2022).

Within this context, my GSM-feature phone device did not seem powerless, quite the opposite. It appeared as a tool that neutralised the harm, to my persona and towards others. I could be trusted, as I had nothing to hide. Anyone could pick up my phone, unlock it and see my texts and calls. No sensible biometric data were stored, and no sensitive data were needed. In fact, my obliviousness to my phone's whereabouts led me to lose it on repetitive occasions. The notoriously harmful perspective of the Fear of Missing Out (FOMO) syndrome resolved itself with the sudden realisation that there was not much that I was missing out on. Or better, that more could be achieved, with less. My feature device was an object that simply had no appeal and no value – nothing much to store and nothing much to hide. Less precious data, minor menacing capta. And by that, again increased considerably my sense of belonging to the people surrounding me and indifference to other more expensive, more problematic, more time-consuming and potentially harmful tools.

'Dumbphone' vs covidiots

With the outbreak of the Covid-19 pandemic in early 2020, the 'successes' of my offlife engagement (reduction of Internet interaction, screen time and online purchases), that I directly associated with captaveillance, became problematic. Since early 2020, in concomitance with the harshening of the virulence restrictions, I could no longer rely solely

on newspapers, cash money, hard-copy entertainment or media in general, as I had done, with some difficulty and great satisfaction, until then. Emergency social isolation and restrictions made the digital world an inevitable portal to access and engage with all information, media, transport and transaction. In the name of health hazards, finding a digital compromise has clearly been a necessary price to the grounded ideas of digital resistance (Lavorgna et al., 2021). With the Covid Digital Certificate and contact-tracing solutions, the 'smart device' I addressed as 'captivating' device became a pivotal tool for hazard monitoring and social hygiene (Csernatoni, 2020). Big Data, with its problems, turned out to be essential to detect threats and potentially future outbreaks (Rathinam et al, 2021) – to the extend of conceiving a neologism of 'coronoption' (The Economist, 2020). In these terms, alternatives proved counterintuitive and were addressed by the socially stigmatising epithet of the 'Covidiot' (Trottier et al., 2021), embedded in the hate scrolling of those who did not abide by the newly established social rules. The feature phone that I was using, short of tracking features and sensors, became evidently a controversial and unjustified gizmo to strangers and institutional eyes. My innocent 'dumb phone' that was once started with curiosity, and at times pity, became transmogrified into a dangerous device of dissidence.

Nevertheless, the problematics that I traced in the replete scenario of onlife captaveillance have become ever more significant. Corporations and state agencies, through contact-tracing apps and the Covid Vaccine Certificates, proved extremely efficient and influential in using 'captivating' elements to control and 'lower the curve' of Covid infections (Sweeney, 2020). Contract tracing was used in practically all affluent societies (Floridi and Sotgiu, 2021). Contact-tracing apps have been promoted as a necessary citizen moral obligation for 'everyone with a cell phone' (Talesnik, 2021). Through these apps, the implication is that the more citizens comply, the better such tools function. Yet, beyond initial crash incidents (underlining that the formula 'more downloads, better service' was not really the case), these Apps have become central elements for the control and monitoring of the virus and its 'carriers' (Gasser et al., 2020). With Covid-19, the capta-dynamics have become pivotal in halting the virus: gathering health data via apps, but also offering immediate and highly effective surveillance practices of 'public health surveillance, urban security, and workplace surveillance' (Trottier et al., 2021: 109). The smartphone could trace the citizens, track their movements, but also allow the immediate and precise filming and reporting of the quarantine breachers, or general dissidents of the restrictions (The (New York Times, 2021). Resisting the captaveillance during the pandemic contributed to captaveillance itself, including episodes of moral vigilantism and denouncing morally corrupt citizens – reporting parties, crowded encounters, 'out-of-perimeter' or 'family bubbles' rendezvous to the authorities: episodes are easily recalled in countries across the globe. These took place in both active and passive episodes of captaveillance: citizens were passively monitored, and they actively monitored each other.

In Italy – one of the notoriously most casualised and restrictive European countries during the pandemic – Foreign Minister of the time Luigi Di Maio expressed dismay towards whoever was reluctant to use contact-tracing apps. Di Maio argued 'ironically' that corporations have been using our data for the past decades with hardly any user being worried (Fatto Quotidiano, 2020) – thus it was a natural predisposition to give up

Data for the greater good. This rhetoric of privacy as a red herring during Covid-19 (Lyon, 2020) is reminiscent of the 'privacy is dead' claim made already 1999 by Sun Microsystems CEO Scott McNealy, who suggested users to 'get over it' (Sprenger, 1999). Such argument comes almost hand in hand with the recurring argument, 'If you have done nothing wrong, you have nothing to hide', which has not only been hardly criticised by the UK Biometric and Surveillance Camera Commissioner Fraser Sampson (2021) but proved quintessentially problematic during the pandemic – whereas the standards of what is wrong and what right may shift so suddenly and abruptly, and previous consent losing suddenly validity. However, this was not at the time nor should today be a justification for mindless techno-fatalism, denying 'the importance of protecting personal data from unwanted surveillance or control from the government or big tech companies' (Lavorgna et al., 2021: 37). eHealth Data may potentially turn into yet a further powerful currency of opaque capta functioning (Pasquale, 2015), as interestingly highlighted already in 2017 in an intriguing volume edited under the name 'Under Observation' (Adams et al., 2017).

Practices of resistance to these forms of surveillance practices, no matter how morally ambiguous and socially harmful in different circumstances, are still today in constant debate (Lavorgna et al., 2021). To resist a form of technological harm, or a 'zemiosis', in the words of Wood (2022), during the Covid-19 crisis has become, it seems, yet again an instance replicating unwanted harm. One had to choose the lesser evil (Williams and Dienes, 2021).

Indeed, the point of how 'capta' may be wrongfully gathered, especially so under exceptional circumstances, is well reported (see Kitchin, 2020; Lavorgna et al., 2021). Luciano Floridi himself, interviewed by Simona Sotciu (2021), noted not only the recurring dangers of the breaching and hacking of highly sensitive health data inefficiently stored by governments and health agencies, but also how these very governments have promoted strict technological discrimination towards whoever is not familiar or even is indisposed towards the technology. The digital health frontier, once a highly debated feature in guaranteeing a delicate balance between surveillance and discrimination (Lombardo and Buckeridge, 2007), within the m-health systems and 'metaverse' realities, are forming the norm for our future interaction in the onlife. For citizens and scholars, this reality turns into a further element of difficulty and indisposition: not only our privacy, but our sense of control faces recurrent and influential means of coercion and harm – social, corporate and institutional.

The appearance of disappearance

For 5 years, I attempted a form of offlife friction that would loosen the 'vigilant' grip of the onlife. The suggested solution, promoted with my auto-ethnography, was to attempt an offlife subcultural existence, even if only partially. My aim was to experiment with ways of 'life' that did not produce endless content and 'capta' food. My solutions were mostly practical, mixing obfuscating software with physically self-limiting my digital engagement.

However, it became very quickly clear that smart devices, phones in particular, were particularly efficient in 'capturing' attention, not only data. Everything in it is designed

to lock you to the screen – pick it up as often and as long as possible. While this sounds trivial, it becomes particularly impressive and truly demanding when attempting to 'opt-out'.

It has been suggested that the digital scenario itself offers ideal conditions for a denial of responsibility, as a 'result of forces beyond their control' (Brewer et al., 2019: 5). My personal choice of no longer 'giving' data could have resulted in a micro-resistance in the system, proving that, partially, some of this may be possible. With Covid-19, captaveillance proved important and beneficial: it protected citizens by tracing their whereabouts, and it offered 'safe and quick' transactions through contactless payments. It has safely delivered groceries and goods. However, even before Covid-19, I noticed that my non-conformity was at best reluctantly tolerated by those fully engaged in the onlife scenario. With my choice of resisting captaveillance, what I seemed to be proposing was an alternative of voluntary 'social isolation', to which no user would abide: Deleuze's assemblage takes over restlessly (Angwin, 2014), though with a purpose. As I have discussed, such oblivious control and permanent authentication are very well represented by smart devices, with our constant online and offline identification (see credit cards and the likes). Inspired by Agre, my conception of captaveillance comes to consider a further element: capturing as an effortless and lax practice. It is not a practice of control: it is a constant and incessant gathering of capta, and a unilateral one. It does not need coercion; it naturally and automatically engages in cohesion and dependence (Han, 2015).

Such consideration brings possibilities for further study, over the criminalisation of this kind of resistance – or indeed, specific instances and occurrences for the securitisation of data. This also requires further work on policy work, analysis and design of platforms and devices currently in use. In the time being, we can rely on platforms, software and add-ons that can scramble, obfuscate, limit and confuse our data – we can decide to opt out (semi) drastically, or struggle to maintain our captaveillance at bay. However, on a final note, once you play by the rules, going back is as hard as ever. Contactless payments are impressively swifter, simpler and by now socially accepted rather than cash. Clicking 'accept' on a website and when downloading an app is undeniably easier and more convenient than opting out – or not using it all. And convenience is often trivially associated with a progressive better, clearer and faster functioning for all of us. From this perspective, one can only slowly realise that although I was looking at corporate responsibility and the harms involved in capturing information, my research in 'disappearing' from the system 'appeared' instead ethically troubled. I was being inconsiderate to the dynamics of distress my approach generated towards others: it was them sensing my actions as problematic. My alternative did not prove a real alternative. Already before Covid-19, I had noticed how my offlife approach appeared unsensible and anachronistic. It seemed to create greater friction in the short term in societal values than in the technologies themselves. By the middle of the pandemic, participating in capta-dynamics was truly a necessary condition that allowed very few if any alternatives. Captaveillance, it would seem, by now is truly the norm.

Conclusions: The cost of capta

It is uncertain how long GSM mobiles will be compatible with current antennas (Wasserstein, 2021), and whether the so-called feature phones will be accessible on the market – not to mention the use of 'cash', the non-conformity to social media, and the refusal to abide by professional metrics, digital citizenships and the likes. One would need to deploy even more tools, 'obfuscation' manoeuvres – forms of sousveillance and whatnot. To attempt to 'disappear' to this neo-normal system would seem to be even more controversial, impractical, and even anti-social. The pandemic has evidently proven so. As noted by *The Guardian* columnist Jen Wasserstein (2021), the 'luxury' of living without smartphone is since Covid-19 harder than ever. The number of smart devices has thrived, and concepts such as digital citizenship have achieved overwhelming significance in the government's bureaucratic establishment. Also, capturing users' whereabouts and encounters has been in fact effective in a moment of a health crisis.

However, this comes at a price. Other than the element of capturing even more information from users and citizens, the protection of information was accompanied with evident flaws (Floridi and Sotgiu, 2021), abuses and security breaches (Lyon, 2022); This becomes even more significant when the information recollected is triangulated, as with the Covid passports, among health, revenue, and immigration statuses (Gasser et al., 2020). Elements of harm and abuse become even more evident in the hands of the beholder, and we may perhaps indulge in the luxury of trust in the Global North, but not so much in other parts of the world. Since Covid-19, elements of captivating technologies again recall the Deleuzian aspects of control when we look at the exclusion, the marginalisation of those who are 'outside' the system (Calzada, 2022). Stateless citizens, liminal individuals, who may not, or do not, wish to be integrated into the capta-grinder become punished and further subjugated. Captaveillance returns with its targeting and insisting scenario (Wiener, 2020). Handing out information in this scenario is promoted not only as a lucrative exercise but as a civic duty. Cohesion yet again oppresses coercion. Resistance, it seems, becomes itself harmful. Desistance, deviant.

Acknowledgements

I vividly thank Fergus McNeill's comments on an early draft of the article and the anonymous reviewers for offering such profound insights.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Janos Mark Szakolczai https://orcid.org/0000-0003-0535-4994

Notes

1. I thank one of the reviewers of the article in framing so well this central distinction.
2. This point is inspired by Agre (1994) article, though the connection data vs capta is not present in the article.
3. One particularly helpful extension, AdNauseam, is promoted and developed by Helen Nissenbaum, offering a tool to 'fight back unilateral surveillance'. Functioning is not simply an 'add-block' feature (limiting the view of an advertisement on a webpage), but scrambling the 'real interest' of the user by clicking literarily all advertisements contained in a webpage. Such a tool comes hand in hand with another related extension, TrackMeNot, that creates a 'bot' of random and incessant searches to scramble the user profile.
4. http://trackmenot.io/faq.html#random
5. My act was evidently perceived as a 'hipster' or 'smug' thing to do – basically an excuse for bringing attention to myself, or demonstrate some sort of 'peculiarity'. Being without social media, especially Facebook, is not the centre of this article; it rather seemed as common sense to me at the time. The birth of my first daughter in 2018 reinforced the desire to increase my capta engagement. For the abovementioned reasons, now less than ever I wished corporations to know the details, store the pictures or speculate on this new existence.
6. The name of the model is not particularly important, as any 'feature' phone offer similar characteristics of the ones described.

References

Adams S, Leenes R and Purtova N (eds) (2017) *Under Observation: The Interplay Between Ehealth and Surveillance*. Berlin: Springer.

Agamben G (2009) *What Is an Apparatus?* Stanford, CA: Stanford University Press.

Agre PE (1994) Surveillance and capture: Two models of privacy. *The Information Society* 10: 101–127.

Angwin J (2014) *Dragnet Nation a Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: St. Martin's Press.

Bauman Z and Lyon D (2013) *Liquid Surveillance*, 1st edn. Cambridge: Polity Press.

Beer D (2016) *Metric Power*. London: Palgrave Macmillan.

Beer D (2017) Algorithms: The villains and heroes of the 'post-truth' era. *OpenDemocracy*, 3 January. Available at: https://www.opendemocracy.net/en/digitaliberties/algorithms-villains-and-heroes-of-post-truth-era/ (accessed 9 October 2021).

Beer D (2022) Why the metaverse will never happen. Available at: https://davidbeer.substack.com/p/why-the-metaverse-will-never-happen (accessed 22 October 2022).

Biddle S (2022) Facebook engineers: We have no idea where we keep all your personal data. *The Intercept*, 7 September. Available at: https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/ (accessed 10 October 2022).

Brewer R, Fox S and Miller C (2019) Applying the techniques of neutralization to the study of cybercrime. In: Holt T and Bossler A (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham: Palgrave Macmillan, pp. 547–565.

Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT Press.

Calzada I (2022) Emerging digital citizenship regimes: Pandemic, algorithmic, liquid, metropolitan, and stateless citizenship. *Citizenship Studies* 27: 160–188.

Chippindale C (2000) Capta and data: On the true nature of archaeological information. *American Antiquity* 64(5): 605–612.

Christl W and Spiekermann S (2016) *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Vienna: Facultas

Csernatoni R (2020) New states of emergency: Normalizing techno-surveillance in the time of COVID-19. *Global Affairs* 6: 301–310.

Deleuze G (1992) *Postscript on the Societies of Control*. Vol. 59. Cambridge, MA: MIT Press, pp. 3–7.

Deleuze G and Guattari F (1987) *A Thousand Plateaus*. Minneapolis, MN: University of Minnesota Press.

Douglas M (1950 [1990]) No free gifts. In: Mauss M (ed.) *The Gift: The form and reason for exchange in Archaic societies*. New York: Routledge, pp. ix–xxi.

Ellis DA (2019) Are smartphones really that bad? Improving the psychological measurement of technology-related behaviors. *Computers in Human Behavior* 97: 60–66.

Fard A (2022) Dark patterns in UX: What you should know. *adamfard*, 7 December. Available at: https://medium.com/@adam.fard/dark-patterns-in-ux-what-you-should-know-ffbcf9747756

Fatto Quotidiano (2020) *Coronavirus, Di Maio:* "*Ci facciamo geolocalizzare anche per ordinare una pizza e poi scoppia la polemica per una app falcoltativa*". Available at: https://www.ilfattoquotidiano.it/2020/04/22/coronavirus-di-maio-ci-facciamo-geolocalizzare-anche-per-ordinare-una-pizza-e-poi-scoppia-la-polemica-per-una-app-falcoltativa/5778892/ (accessed 26 June 2023).

Ferrell J, Hayward KJ and Young J (2008) *Cultural criminology: an invitation*. Los Angeles, London: Sage.

Ferrell J (2018) *Drift: Illicit Mobility and Uncertain Knowledge*. Berkeley, CA: University of California Press.

Ferrell J (2022) In defense of resistance. *Critical Criminology* 30: 603–619.

Floridi L (2015) *The Onlife Manifesto: Being Human in a Hyperconnected Era*. New York: Springer.

Floridi L and Sotgiu S (2021) Green pass e hacker, l'italia onlife di draghi vista da floridi. Available at: https://formiche.net/2021/08/green-pass-e-hacker-litalia-onlife-di-draghi-vista-da-floridi/ (accessed 23 October 2022).

Forssell R (2016) Exploring cyberbullying and face-to-face bullying in working life – Prevalence, targets and expressions. *Computers in Human Behavior* 58: 454–460.

Foucault M (2008 [1978]) *The Birth of Biopolitics: Lecturers at the College de France, 1978–1979*. Basingstoke: Palgrave Macmillan.

Garfinkel H (1967) *Studies in Ethnomethodology*. Hoboken, NJ: Prentice-Halls.

Gasser U, Ienca M, Scheibner J, et al. (2020) Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid. *Lancet Digital Health* 2: e425–e434.

Ghita C and Thorén C (2021) Going cold turkey!: An autoethnographic exploration of digital disengagement. *Nordicom Review* 42(S4): 152–167.

Giglioli MF (2019) *I Labirinti della Sorveglianza Informatica*. Milan: Il Mulino.

Haggerty KD and Ericson RV (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605–622.

Han B-C (2012) *The Transparent Society*. Stanford, CA: Stanford University Press.

Han B-C (2015) *The Burnout Society*. Stanford, CA: Stanford University Press.

Han B-C (2022) *Non-Things: Upheaval in the Lifeworld*, 1st edn. Cambridge: Polity Press.

Herrero J, Torres A, Vivas P, et al. (2021) Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International Journal of Environmental Research and Public Health* 18(7): 3763.

Horst H (2020) Friendly social surveillance. In: Hjorth L, Ohashi K and Sinanan J (eds) *Digital Media Practices in Households: Kinship Through data*. Amsterdam: Amsterdam University Press.

Johnson B (2010) Privacy no longer a social norm, says Facebook founder. *The Guardian*, 11 January. Available at: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (accessed 6 November 2023).

Kitchin R (2020) Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity* 24: 362–381.

Lanigan RL (1994) *Capta Versus Data: Method and Evidence in Communicology*. Berlin: Springer.

Lavorgna A (2014) Internet-mediated drug trafficking: Towards a better understanding of new criminal dynamics. *Trends in Organized Crime* 17: 250–270.

Lavorgna A (2021) Looking at crime and deviancy in cyberspace through the social harm lens. In: Davies P, Leighton P and Wyatt T (eds) *The Palgrave Handbook of Social Harm*. Berlin: Springer, pp 401–420.

Lavorgna A, Rekha GS, Ugwudike P, et al. (2021) To app or not to app?: Understanding public resistance to COVID-19 digital contact tracing and its criminological relevance. *Law, Technology and Humans* 3: 28–45.

Lovink G (2019) *Sad by Design: On Platform Nihilism*. London: Pluto Press.

Lowry PB, Zhang J, Wang C, et al. (2016) Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research* 27(4): 962–986.

Lyon D (2018) *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Lyon D (2020) *The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy'*. Available at: https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060 (accessed 26 June 2023).

Lyon D (2022) *Pandemic Surveillance*. Cambridge: Polity Press.

McGlynn C and Johnson K (2021) *Cyberflashing Recognising Harms, Reforming Laws*. Bristol: Policy Press.

Marcum CD, Higgins GE and Nicholson J (2017) I'm watching you: Cyberstalking behaviors of university students in romantic relationships. *American Journal of Criminal Justice* 42(2): 373–388.

Marganski A and Melander L (2018) Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence* 33: 1071–1095.

Marx GT (1998) Ethics for the new surveillance. *The Information Society* 14(3): 171–185.

Marx GT (2016) *Windows into the Soul Surveillance and Society in an Age of High Technology*. Chicago, IL: University of Chicago Press.

Nissenbaum H (2015) Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*. Epub ahead of print 12 July. DOI: 10.1007/s11948-015-9674-9.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Pescovitz D (2009) Missing: Phil Agre, internet scholar. Available at: https://boingboing.net/2009/11/24/missing-phil-agre-in.html (accessed 20 October 2022).

Przybylski L (2020) *Hybrid Ethnography*. Berkeley, CA: Sage.

Pugliese J (2012) *BiometricsBodies, Technologies, Biopolitics*. Abingdon: Routledge.

Rathinam F, Khatua S, Siddiqui Z, et al. (2021) Using big data for evaluating development outcomes: A systematic map. *Campbell Systematic Reviews* 17(3): e1149. https://doi.org/10.1002/CL2.1149

Redden J, Brand J and Terzieva V (2020) Data harm record. Available at: https://datajusticelab.org/data-harm-record/ (accessed 5 December 2021).

Sampson F (2021) 'If you've done nothing wrong. . .': 5 reasons why this is no defence for surveillance. Surveillance Camera Commissioner's Office. Available at: https://videosurveillance.blog.gov.uk/2021/05/27/if-youve-done-nothing-wrong-5-reasons-why-this-is-no-defence-for-surveillance/ (accessed 20 March 2023).

Selmini R and Chiaramonte X (2022) *La Criminalizzazione Del Dissenso*. In: Pitch T (ed.) *Devianza e Questione Criminale. Temi, Problemi e Prospettive*. Roma: Carocci editore, pp. 243–262.

Shariff S (2014) *Sexting and Cyberbullying*. Cambridge: Cambridge University Press.

Sprenger P (1999) Sun on privacy: 'Get over it'. *Wired*. Available online at: http://www.wired.com/politics/law/news/1999/01/17538 (accessed 26 June 2023).

Sweeney Y (2020) Tracking the debate on COVID-19 surveillance tools. *Nature Machine Intelligence* 2: 301–304.

Talesnik D (2021) Privacy in Pandemic: Oxford Professor Explores Ethics of Contact Tracing. NIH Record, 21 05. LXXII(3).

The Economist (2020) Creating the coronopticon. The Economist, 26 May. Available at: https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic (accessed 4 December 2021).

The New York Times (2021) German intelligence puts coronavirus deniers under surveillance. *The* New York Times, 28 April. Available at: https://www.nytimes.com/2021/04/28/world/europe/germany-coronavirus-deniers-surveillance.html?action=click&module=Top%20Stories&pgtype=Homepage (accessed 4 October 2022).

Tokunaga RS (2011) Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. Computers in human behavior. *Computers in Human Behavior* 27(2): 705–713.

Trottier D (2019) Denunciation and doxing: Towards a conceptual model of digital vigilantism. *Global Crime* 21: 196–212.

Trottier D, Huang Q and Gabdulhakov R (2021) Covidiots as global acceleration of local surveillance practices. *Surveillance & Society* 19(1): 109–113.

Vaidhyanathan S (2012) The cryptopticon: The legal, ethical, and intellectual implications of 'big data'. *College of William & Mary Law School: Mervis Lecture*. Available at: https://scholarship.law.wm.edu/mervis/1/

Vaidhyanathan S (2018) *Antisocial Media*. Oxford: Oxford University Press.

Vertesi J (2015) How evasion matters: Implications from surfacing data tracking online. *Interface* 1: 2373–4914.

Wasserstein J (2021) My life without a smartphone is getting harder and harder. *The Guardian*, 4 Thursday. Available at: https://www.theguardian.com/commentisfree/2021/nov/04/my-life-without-a-smartphone-is-getting-harder-and-harder#comments (accessed 25 August 2022).

Wiener A (2020) Taking back our privacy. Available at: https://www.newyorker.com/magazine/2020/10/26/taking-back-our-privacy (accessed 5 March 2021).

Williams SN and Dienes K (2021) Public attitudes to COVID-19 vaccines: A qualitative study. Available at: https://www.medrxiv.org/content/10.1101/2021.05.17.21257092v1

Winkelman BS, Oomen-Early J, Walker AD, et al. (2015) Exploring cyber harassment among women who use social media. *Universal Journal of Public Health* 3(5): 194–201.

Wood MA (2022) Mapping technology-harm relations: From ambient harms to zemiosis. *Crime, Media, Culture* 18(4): 509–526.

Yar M (2005) The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology* 2(4): 407–427.
Zuboff S (2019) *The Age of Surveillance Capitalism*. London: Profile Books.

Author biography

Janos Mark Szakolczai is a Lecturer in Criminology at the University of Glasgow. His work focuses on the hyper-vigilance of intimate spaces, particularly toxic and covert elements of coercion and control via devices. He has recently led a Scottish Government funded research project on public space CCTV in Scotland.