Yet another prying eye
Surveillance as a consented cultural phenomenon?

Ricardo Rodrigues de Oliveira[*]

PhD researcher at the European University Institute, Florence

SUMMARY

[*] PhD researcher at the European University Institute (EUI), Florence. Assistant Researcher to Professor Deirdre Curtin and Researcher of the Centro de Investigação em Direito Público (CIDP-ICJP) of the University of Lisbon School of Law (FDUL) and of Jurisnova of the New University of Lisbon School of Law (FDUNL). The section "A normal day" was originally presented in the seminar "Information Technologies and Fundamental Rights through the Cases", organized by professors Deirdre Curtin and Giovanni Sartor, that took place in the Spring semester of 2017, at the EUI. This is the consolidated paper developed after the presentation of the draft work at the Católica Graduate Legal Research Conference 2017 "Law in the Era of Technological Change", that took place on the 21 and 22 September 2017, at the Lisbon Campus of the Portuguese Catholic University School of Law. My warm regards to the convener of the event, Isabel Teixeira Duarte, to the sharp yet friendly commentator of my paper, Catarina Santos Botelho, and to the reviewers of this text.
Closed Circuit Television (CCTV); Court of Justice of the European Union (CJEU); Global Positioning System (GPS); Internet Protocol (IP); Information Technology (IT); North-American National Security Agency (NSA); United Nations (UN).

“We live in an everyday that is saturated with surveillance. It is a major shift from an earlier era where surveillance was something one experienced in specific places and under the gaze of one person or thing.”[1]

Introduction

Just like Nayar described it, surveillance is no longer concentrated to very contained spaces under the watchful eye of a handful of people. Surveillance is no longer limited to a panopticon-like tower – it is a true “surveilling assemblage”. The model suggested by Jeremy Bentham no longer describes the surveillance *status quo* because it’s too neat and straightforward. Two traces that seem absent in the processing of personal information in modern times, where blurred mass surveillance reaches everyone and everything.

Nonetheless, the United Nations (UN) have systematically affirmed[2] that a person’s right to privacy forbids arbitrary or unlawful interference. Any violation should be sanctioned by law, in line with Articles 12 of the Universal Declaration of Human Rights[3] and 17 of the International Covenant on Civil and Political Rights[4].

This can strike an external onlooker as rather odd. In this clash between muddled surveillance and the forthright resolutions of the UN, what prevails? Considering that most surveillance systems, formal or informal, are effective more by the “lingering threat” that individuals might be under their gaze rather than being actually monitored[5], modern technologies can threaten the exercise of every individual right and freedom.

[1] Nayar (2015), p. 6.

[2] It was most recently included in the first articles of the UN’s Resolution of the General Assembly A/RES/71/199, adopted on 19 December 2016 (65th plenary meeting), and of the Resolution of the Human Rights Council A/HRC/RES/34/7, adopted on 23 March 2017 (56th meeting). This is a renewal of prior texts, namely the Resolutions of the General Assembly A/RES/69/166, adopted on 18 December 2014 (73rd plenary meeting), A/RES/68/167, adopted on 18 December 2013 (70th plenary meeting), and A/RES/2450 (XXIII), adopted on 19 December 1968 (1748th plenary meeting). It had also been addressed in the Resolutions of the Human Rights Council A/HRC/RES/31/7, adopted on 23 March 2016 (62nd meeting), A/HRC/RES/28/16, adopted on 26 March 2015 (28th session), and A/HRC/RES/26/13, adopted on 26 June 2014 (38th meeting).

[3] Which reads that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks”, according to the Resolution A/RES/3/217 A (III), adopted on 10 December 1948 (183rd plenary meeting).

[4] This Article, part of the annex of the Resolution A/RES/21/2200 (XXI), adopted on 16 December 1966 (1496th plenary meeting), copies the text of the Universal Declaration.

[5] Irion (2015), p. 81.

Watchful technologies seem to be creeping into our daily lives. They are becoming a part of what it means to live in cities and to interact with others. They are turning into an element of our modern cultures and we can no longer live without them. However, most of us seem "intolerant" to them when we realize how much a random day can be populated by technologies that monitor and register our movements. There is a difficult appeal to compromise here. This paper addresses the notion of consent as key to understand our social behaviors, thus explaining the phenomenon we are experiencing.

This research aims precisely at reflecting on what's happening regarding surveillance from a composite standpoint: it puts together legal analysis with technological and sociological reasoning. It is not aiming at solving problems – it is up to authorities and agencies to ponder on the ideas presented here and turn them into action. As such, there are two main goals in this paper, besides clarifying the modern "surveillance reality". The first is to explain how and why surveillance is crawling (and not even on tiptoes) into every aspect of existence, from governmental programs to personal affairs. Through the concept of consent, seldom used in related literature, this paper will probably come closer to more accurate answers. The second, shaped as the main conclusion, is a suggestion for a brighter future. Considering that certain facts will remain regardless we like them, it is through introducing surveillance techniques in the sustainable development discourse that we can arrive at a better social environment. This does not amount to confusing matters, namely hard and human sciences; because sustainable development has a social side and surveillance, data protection, privacy, and the use of technology are very much key elements in out societal modern lives. Accountability, transparency, and preemptive scrutiny are just some of the components that will make present and future surveillance apparatuses sustainable in our communities.

This work is divided in 5 sections. It begins by illustrating a random day to make the reader grasp the perspective guiding the argument. Then it engages with the concept of surveillance and introduces some reasoning of using monitoring apparatuses in the public discourse. The following part tries to briefly deconstruct the persistent nothing-to-hide argument and makes the bridge to the private use of surveillance, a section which highlights some of the perils of trusting and consenting to commercial policies. Finally, my research into consent becoming a cultural feature of modernity is dealt with in the last segment. The main argument, as mentioned before, is that surveillance is not an inevitability but a useful tool that should be wielded sustainably. In fact, sustainability is the "unexpected" answer in a project that started looking only at the problem but that later aspired to move further towards a solution.

A normal day

In our daily lives, it's hard to avoid being under the prying eye of any technological gadget[6]. Just like in Stephen King's *Under the Dome* novel of 2009, the idea of an "omniscient eye of the Supreme Being" is present in the form of technical surveillance in the 21st century because human beings have an obsession for watching and spying one another[7]. As I am writing this text, I am well aware that the internal camera on my computer is pointing directly to my face. Its silent gaze menacingly remembering me that someone can be watching behind that little dark circle, almost imperceptible in the black framing of the desktop. In fact, its invisibility is almost a cynical metaphor for what might be happening in the shadows of the electronic circuits connecting my MacBook to someone sitting halfway across the globe in Cupertino, California. And I suspect it's not only when this dot prickles to life that they might see me. Whoever *they* may be.

Let's picture a random day to get a sense of some Information Technologies (ITs) that can be used to trace our steps daily – just to put things in context and with no intention of exhaustion. You wake up and snooze the alarm clock of your smartphone – this is one of the most obvious tracking devices that comes to mind as we can no longer live without these tiny computers. Smartphones are incorporated with a Global Positioning System (GPS) microchip that is constantly active, even if the device is disconnected. Some systems allow for the disabling of the location caching[8], but other don't. Or make it harder. Numerous web forums discuss the relentless quest for GPS service by some apps, even if not directly concerned with navigation functions. From weather forecasts to restaurant hints, the fact is that sooner or later you're bound to turn your location system on again, making big brother resume its faithful activity of being on to you.

Phones have normally inset also both a camera and a microphone, used so often for vocally WhatsApp – an app like so many others that have requirements for proper functioning, like checking your location or connecting to a mailing account. Either way, whenever you move or log in, the system will know and the information will go to a main server. All these technologies can tell you, and someone else, where you are, what you see, and what you say. And you haven't even showered yet.

While taking breakfast you probably have the television on to check the morning news. The most recent TVs can be (optionally) connected to the

[6] A futuristic and more unsettling account than the one described here can be found in the engaging lines of Tudge (2010), pp. 11 ff.

[7] Nayar (2015), p. 2.

[8] Gordon (2011).

internet. Your provider will know you turned it on and what you decided to watch to make a commercial profile and draft a channel audience share. This enables the company to personalize your newsletter to specific needs, either yours or theirs. Live monitoring through the "idiot box" can also happen when you have a model with an embedded camera and microphone.

Certain people tape every piece of hardware to block unwanted viewers and muffle sound-recording. The rate of success is, obviously, unknown and unaccountable. Computers are some of the best examples of this; they are obvious devices when it comes to e-surveillance. Practically everything we do related to study, businesses, or social life involves computers and phones. You will turn your computer on during the day and be sure to leave a record behind you. Even if you delete it regularly, some programs remember your every keystroke, keep your passwords, and report on technical errors — but some will unsuspectedly and politely ask you first.

If you use your company or university's device, there will be an IT guy potentially surveilling or controlling it from an ethereal room hardly anyone has paid a visit to. You will remember him only when the system crashes but he will know what you do whenever he feels like it. When using an institutional card, the data administrators/controllers will also know where and when you've been and if you have the right to open this or that door. But it's not only at your workplace these cards exist: at the gym, the swimming pool, or the unsuspected supermarket.

To withdraw money from an automatic machine, you need clearance and approval from your Bank. It will obviously know when you need some extra funds in your pocket or decide to pay anything with a card. The banking and automated teller machine systems will generate a response to your request according to the account settings and other conditions. Usually, a Closed Circuit Television (CCTV) resembling the little circle on my computer or in the shape of mirror-like metals is placed on every machine for your safety and security. Remember to smile as someone might be smiling back.

Public (and more and more private) enclosed systems for surveilling through video cameras are the most visible means of monitoring. They are usually at the core of fora on public security policies. CCTV exists since 1942[9]. Today, it is the prototype of technologically organized monitoring[10], being widely spread in every metropolis, whether inside[11], at the doors of buildings, or in the streets.

[9] Tudge (2010), p. 83.

[10] Leman-Langlois & Larivière-Bélanger (2011), p. 157.

[11] There is yet little empirical evidence on surveillance in certain mixed (both private and public) areas such as schools but, according to Taylor (2012), pp. 228-229, the few studies conducted on surveillance there have shown it "undermines privacy, erodes trust, makes pupils feel criminalized and can have a 'chilling effect' on creativity and interaction".

Depending on where you live, your days can be reconstructed based on digital images recorded by CCTV alone. London is the most "spied-on city in the world", topping New York and Beijing, with approximately 51,000 cameras, mostly located at the entry points of the capital's core[12].

Getting home can be an exercise in surveillance as well. Apart from cameras in public buildings, hotels, shopping areas, stadiums, museums, banks, main avenues and squares, public transportation are required to have inbuilt cameras. If they don't, your monthly pass has a microchip that can be used to trace your whereabouts[13]. And if you walk home, you can get caught in anecdotal ways. Imagine Google Maps is updating their data or a drone is flying by to make a breathtaking video for some advertisement. Be careful not to be in the wrong place at the wrong time.

At home, you go online through your highly-suspicious (yet taped) computer. The only real guaranty when accessing the internet is probably e-surveillance. Facebook, for instance, declares that they "are passionate about creating engaging and customized experiences for people", *i.e.*, looking what you are up to. For that, they collect: *i*) things you do and information you provide; *ii*) things others do and info they provide; *iii*) your networks and connections; *iv*) intelligence about payments; *v*) device data, namely attributes, location, and connection; *vi*) input from websites and apps that use their services; *vii*) info from third-party partners; and *viii*) something else from their own companies. As the Nespresso ad goes, what else?[14]

If you decide to go on a short trip to get away from all these meddling ITs, big brother will go along[15]. To make it simple, you decide to check flights online

[12] World Atlas (2017). According to Lloyd (2011), p. 6, there are about 4.2 million CCTVs operating in the United Kingdom, about a quarter of global installations, which makes an average of about one camera per 14 inhabitants, and it is estimated that a person can be "caught" on camera about 300 times a day. For an account on the growth of CCTV in the UK and other countries in Europe, see Norris (2012), pp. 252 ff.

[13] According to Lloyd (2011), pp. 3-4, London's "Oyster cards" have been one of the main sources of information for law enforcement agents in this metropolitan area, particularly for the long time-span of eight weeks during which the commuters' journeys are recorded and the fact that some of these passes carry the user's personal identification. To make people adhere to this data-collector system, the transport authorities even raised the price of paper tickets and lowered that of such cards, creating a true monopoly of access to public transportation in the city [Tudge (2010), pp. 89-90].

[14] According to Thelwall (2013), p. 75, internet content can be less ephemeral than first thought regarding personal information and communication as much online material is copied into the Internet Archive, available at archive.org (11.10.2017), or similar databases, namely those created by the website owners or administrators. Facebook, for instance, stores deleted profiles and retains them as suspended until activation by the user for, allegedly, marketing purposes.

[15] A barely novel yet still controversial technology that can also come along are radio frequency identification structures. These consist of implanting nano-microchips under the skin or in personal belongings containing personal data and a tracking system. Some can transmit a radio frequency, while others need scanning to be read. They are widely used most for geo-locating shipping orders but debates have arisen when they become mandatory for certain populations. See Tudge (2010), p. 89.

from aggregating platforms or directly from carriers' websites. Obviously, the point of departure is automatically filled because *they* suspect the airport you will be using, either from previous trips or because it's the closest to your actual location. Perhaps the prices are still a little too expensive and you create an e-alert to know when they will lower. You don't even pay attention and end up signing to the website's newsletter.

Five minutes later you check in on Facebook again to see what someone else is up to. And to leave some transient trace that will, somehow, be made permanent[16] without your awareness. What will you get on the right-side column? The one with the advertising… The analysis of a person's connections to other people, goods, and services permits software to make inferences about attitudes, taste, desires, and aspirations. As expected, what you get is "virtual nudging" about that trip you're planning. Because someone knows you want to go somewhere, someday.

IT surveillance in the public discourse

Surveillance – to "watch over" from its original French – is a routine attention to specific features for influence and control[17]. It involves collecting data, processing it, and interpreting the results. Nowadays, usually big data[18]. IT surveillance refers specifically to monitoring by means of electronic devices. In the arrangement of physical, physiological, and data surveillance[19], technological monitoring would be an example of this last group. Surveillance does not depend on technology, unlike Tudge (2010), p. 83, claims, but technological apparatuses are more and more being used in monitoring routines and surveillance is increasingly becoming associated with technology.

Technology is expanding and blurring the boundaries of surveillance. So, perhaps an updated and useful distinction would also be between direct (targeted)

[16] One of the many "troubles" of social media surveillance, for Trottier (2012), p. 7.

[17] Lyon (2007), p. 13. Elsewhere, Lyon (2001), p. 56.

[18] Big data is not only the clutching together of large quantities of information. Lyon (2015), p. 69, argues that it's also a way of managing data, as well as the twists and turns they may go through. How big databases are arranged, and how they are used and consulted, is different from smaller catalogues. The idea of big brother is associated with this novel manner of looking at data and metadata for the conclusions that can be drawn from the immense variety of links, even if only speculative, connecting the thousands of entries – it's certainly a new trend in the configuration of power. Also, in general, Ho, et al., (2017).

[19] Lloyd (2011), p. 4.

surveillance[20] and the "more general, all pervasive surveillance which permeates all our lives without being specifically directed at any particular purpose"[21].

Different tools and agents are tasked with the several sections of the surveillance process. The collection of data is the most visible facet of the chain of information – the scrutiny that makes citizens feel they're losing privacy[22]. The other two typically remain "hidden" and abide by technical criteria that "secretly" conduct a form of social sorting. This can be of a general nature – the random monitoring by just looking at individuals' external traits – or follow precise guidelines. On the latter, Lloyd mentions the city council installation on London's borough of Newham aiming specifically at matching passersby with databases of known offenders. Apparently, there is a rate of 75% accuracy, with some claiming this system to be sophisticated enough to overcome most attempts of facial and identity concealment. The next step in these CCTVs has been the programmed testing for behavioral patterns that might be found suspicious.

The author alerts, however, for the devious side of such systems and the mindset behind them, well embedded in the "normalization" of spying[23]. It is very hard to measure or quantify how ITs affect individuals personally. Yet, the underlying problem is not exactly that one particular citizen was filmed but that everyone might be surveilled "indiscriminately and without a pre-established reason"[24]. The installation of technology must be proportionate, especially as it is freely accessible worldwide. Political activism has sometimes preferred aggressive measures to make public, visible, statements in the fight against crime and terrorism.[25] Times of insecurity often lead to the radicalization of preventive responses, trumping civil liberties under (stagy) public concerns. The system in Newham, for instance, relied on no less than 150 cameras, making a large percentage of innocent citizens suspect and systematically run against police databases[26].

[20] Lyon (2015), p. 70.

[21] Lloyd (2011), p. 5.

[22] Literature on intelligence and privacy sees collection activities as a first "battling ground" for data protection discussions. For a specific analysis on the debate concerning counter-terrorism and surveillance in international law and human rights, see Chesterman (2014), pp. 454 ff.

[23] Tudge (2010), p. 15. The author illustrates the idea with "intitucionalized" shadow networks of espionage, such as the North-American National Security Agency (NSA), which was only publicly known in the 70s, or the British MI5 and MI6, "unmentionables until the 1990s, with recruitment involving Oxbridge undergraduates being 'sniffed at by wolves'".

[24] Sloot (2017), p. 156.

[25] Surveillance studies usually divide their research interests among the different "surveillance sites", the political and social "areas of intervention" requiring monitoring mechanisms. See, Lyon (2007), pp. 25 ff. Also, Trottier (2012), pp. 17 ff.

[26] Lloyd (2011), p. 7.

The processing of data no longer depends primarily on human agents in some cases[27]. Speed radars automatically process the information retrieved from the license plates of vehicles, verify it against police databases, and flag any violation of the area's speed limit or the emergence of suspect cars. Nevertheless, (so far) there has always been the need for a human intermediary looking at the data, correcting anomalies, verifying the info and the automatic orders, and generally bridging the gaps in terms of profiling. The replacement of humans by fully-automated modules is also an issue on the surveillance debates, particularly those concerned with the accountability of the parties.

Surveillance is a pressing issue in every legal order, as well as in the international sphere[28]. In the global fight against terrorism, IT surveillance has been an all-to-common "weapon" for political ideologies and actors to twist what we consider to be "lawful interception". This has been done by more and more means of formal and informal preemptive monitoring through the retention of bulk data[29]. Can we think of any contemporary city without surveillance? Nonetheless, this is not a new or exclusive phenomenon of modernity. It has happened since there was need to watch and control disruptive forces in the society. Surveillance has met different resistances but one thing is certain now: it's a global condition. A condition *sine qua non* to inhabit cities[30]. A condition to engage in social affairs in the urban landscape. A condition to e-interact – something that is done more and more in urban settings with the development of societies[31]. So, the novelty aspect is that it's no longer just a simple gathering of data for "positive" effects, like law enforcement to check on criminals or for permitting health services to find the best solutions for patients. Commonplace beliefs of surveillance associate it with power and dominion[32], with big data being extracted from citizens, retained in large catalogues, and processed through unknown information systems for the control and tracing of individuals by authorities or corporate bodies. Is *this* accurate?

Although the state has always been inclined to see privacy differently from people, the problem nowadays is that it finally has the tools to enforce its view. Moreover, surveillance is no longer concentrated but dispersed through numerous locations from where data can be collected. And can often be accessed

[27] Ogura (2006), p. 280.

[28] For a study on data protection and informational privacy in international law, jurisprudence, and state practice (through a human rights-based comparative assessment) see, *inter alia*, Rengel (2013), pp. 145 ff.

[29] Irion (2015), p. 80.

[30] Fussey & Coaffee (2012), p. 201.

[31] Lyon (2001), p. 51.

[32] Nayar (2015), p. 5.

by multiple agencies[33] as intelligence is scattered throughout records and databanks – from employment to medical histories, as well as in the form of users' cards, check-ins, or Internet Protocol (IP) addresses. Naturally, the entities collecting and processing such information are multiple. Even if the state was the only harvester, the truth is that it gathers much more and diverse information than it did a couple of decades ago[34].

An interesting dimension of how surveillance is undertaken is precisely the fractioning of the "self-surveilled". There is no single "big brother" anymore. There is an assemblage of private and public, big, and perhaps not so big, brothers and sisters. The expansion of surveillance has led to the specialization of monitoring purposes. The individual can be monitored as a customer, worker[35], consumer, passenger, internet user, cash withdrawer, patient, etc[36]. Even some of these at the same time: imagine going to a shopping center. There are security guards and CCTV that see you as a visitor. The retail shops as a consumer. If you go to a travel agency, they will perceive you as a prospective passenger, as well as a consumer and cash payer. All in the same space but all linked to different centrals of command and processing systems. Getting the data from all these means of surveillance creates a diffuse puzzle made of fragments of a person's whereabouts and undertakings. But the moment it is put together, the image created will have a high degree of accuracy, bringing circumstances, metadata[37], and data into one (big) file extremely useful for tracing.

It might seem harder to trace someone's steps this way but fragmentation means more information. The pieces can be put together and a chronology depict an identity with far more precision. Law enforcement can prove or disprove an alibi in a much more detailed manner than without diffused surveillance. Yet, in times of legitimacy crisis, mass surveillance can easily slide to mass movement control, for political reasons or other. In fact, surveillance by ITs is "the most versatile system from crime control to political management of the population,

[33] A reality worsened by conflicting competences between law enforcement agents and intelligence services in certain countries [Chesterman (2014), pp. 458 ff.].

[34] Nayar (2015), p. 6.

[35] For a hypothetical model of an "omniscient organization", see Marx (2016), pp. 180 ff. The relations between employers and employees have provided important experimental evidence regarding the effects of systematic monitoring practices, which can have a profound negative impact in productivity rates. Drug testing, alongside technological lurking, is a good example, particularly in the US. Curiously, however, most corporations end up not gathering related statistical evidence to demonstrate the benefits of such regular testing on staff wellbeing, defeating the very purpose of such monitoring.

[36] Nayar (2015), p. 7.

[37] Lyon (2015), pp. 73 ff.

as CCTV on the streets as a technology of crime control is easily converted into surveillance of demonstrators on the street"[38].

Surveillance is one side of our social relations[39/40]. CCTV links people and the relations stablished between watchers and watched are something of a trade. A trade in power. This apparently grim depiction of life cannot be underestimated. It can even come to affect democracy. Surveillance in public spaces shifts the balance of speech and the potential exercise of rights in numerous occasions, like on parliaments. It can tilt the balance towards more accountability of people holding official duties but it can also curtail participation in the power processes[41]. Visibility is usually positive for the enforcement of legal and constitutional principles, like transparency, certainty, and security. It reveals corruption, bringing light to opaque procedures. Exposure positively turns the public into the watcher of the state, but one should be cautious about phenomena like WikiLeaks, which might not altogether be beneficial for states' affairs and diplomacy, even on behalf of the security and welfare of citizens.

The way surveillance is implemented is also relevant in the shaping of how we deal with technologies. "Draconian" surveillance, especially if introduced in a top-down approach, tends to meet higher resistance. This term can describe surveillance that surprises subjects because it was not expected or because it was introduced without their participation. On the other hand, it can also relate to a degree of intrusion. The workplace is a good sandbox. There are no work environments that can do without some form of monitoring. Technological surveillance is becoming more and more the norm, with debates nowadays falling on e-mail monitoring and video cameras in "unusual" places, such as working spaces or even locker areas, not to mention toilets[42].

Although monitoring is necessary to maintain order and productivity rates[43], this kind of surveillance in public and private spaces can seriously unsettle individuals, which come to believe their superiors don't trust them. And the fact is that even if there is a stable work environment, surveillance can become itself a disruptive force, breaking the bonds of trust under a layer of suspicion.

[38] Ogura (2006), p. 289.

[39] Nayar (2015), p. 3.

[40] Thelwall (2013), p. 68, asks relevant questions on the balance of social interactions on and offline such as "[d]o people expect more from a life partner met via the large databases of online dating agencies? Are distant relationships easier to maintain over time with Facebook? Do migrants retain closer connections with the birth country if they share family videos on YouTube?".

[41] Nayar (2015), p. 10.

[42] Marx (2016) p. 194.

[43] Even as a general benefit by registering unlawful or devious behavior and making people accountable. It's not uncommon the use of video records as evidence in cases of sexual harassment or theft, for example.

Excessive surveillance triggers precisely some of the behaviors it aimed to halt, like material and "time theft", absenteeism, or production inefficiency. Also, it tends to overpower the feeling of the self[44]. When the watched cannot watch the watchers, these become dangerously unregulated[45]. And those who do not know when and if they're being monitored cannot point the finger at the watcher if he does something wrong himself – or if he is not paying careful attention[46]. Certain feelings tend to grow *viz.* excessive surveillance mechanisms[47], like demoralization, disrespect, or anger. And the more draconian, *i.e.*, the more intrusive and surprising, the more this sense of dehumanization will develop.

Nothing-to-hide

A common response to counter-balance privacy is the nothing-to-hide argument. Or slogan[48]. For the advocates of "borderless" truth, the complexity of modern life prevents enforcing the rule of law unless individuals are made "transparent". Stripping the individual of clothes, secrets, or possessions, and laying him in the "open" is, for them, the only way in which preemptive security can operate to a full efficiency degree. And if the person has nothing to hide, it won't matter because her privacy will be restored as soon as possible. Or convenient.

Although barely reasonable from a human rights' perspective, this need to put up with private and public meddling still strikes many as plausible. In fact, counter-terrorism strategies used to ignore human rights[49] and data protection commitments. The main issue here, however, can be demonstrated by a simple

[44] Most services provided online demand personal information or are somehow linked to services and tools that feed them with users' data. That's why it can be an interesting exercise to go on "vanity searches", *i.e.*, to Google yourself, and perhaps your family and friends. This is the price of access to knowledge: to provide our own knowledge to others, even if we're not a public figure – and there lies the root of the trade in power. This "dark side" is illustrated by the most-used research tool online: Google and Google-owned software register digitalized data and locate it online through our IP addresses or, in the case of dynamic IPs, through our browser details listed by websites' cookies. See Guarda (2009), pp. 250-251.

[45] Tudge (2010), p. 86.

[46] Plus, the possible scenario of bad, outdated, or broken systems that sometimes do not help identifying the perpetrators at all.

[47] Marx (2016), p. 194, mentions an empirical research by Smith, *et al*., 1992, among others, that are quite revealing of the average greater stress and dissatisfaction levels felt by employees under monitoring when opposed to non-monitored workers.

[48] In general, Solove (2013).

[49] Even at the UN level, only in 2005 was established the mandate of a Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. This was pushed through by the Resolution of the Commission on Human Rights 2005/80, adopted on 21 April 2005 (60th meeting), which later would lead to the UN's Resolution of the General Assembly A/RES/60/288, adopted on 8 September 2006 (60th session). See Scheinin (2013), p. 582.

understanding of privacy as a core legal value. The right to privacy has a negative side, which, broadly, consists of keeping people outside of one's personal business. For the full enjoyment of this right, all it takes is a quiet *erga omnes* daily experience of…being left alone. In fact, a fundamental right should never be perceived as a permanent defense that the individual must wield constantly to demonstrate being on the right side of the law.

Embedded in the very fabric of every legal system based on sound principles is the straightforward presumption of innocence. Any democracy would be perverted if the citizen had to demonstrate his innocence and not the accusers his wrongdoing. To ask for considerable exposure under the idea that, otherwise, he or she has something to hide, makes suspicion preclude privacy. Saying that people will only be innocent if they have nothing to hide shifts the focus of law and principle from one's inherent human rights to mechanical and malicious suspicion, to an ever-present doubt that displaces the human being from the center of the legal system. In the end, this would most likely turn into a *carte blanche* to (more) aggressive governmental surveillance. To inconceivable control. To less-than-democratic oppression.

This reasoning is preoccupying not only in the public space. In the workplace, paranoid employers would be tempted to find "disloyalties" from their staff, preemptively jeopardizing privacy by abusively intruding into people's lives. And the "meme 'nothing to hide, nothing to fear' might then be applied to them, leaving them suspected of anything from a drug habit to an affair"[50] – which are outside-of-the-job behaviors that should not be used to endanger the work position of any employee, except in very specific circumstances. In fact, workplace surveillance is big business but not necessarily also good for business[51]. If this is yet not convincing enough, picture yourself getting arrested on the street[52] or doing some less-than-social behavior like peeing outside. Now, picture this while getting caught on a 360.º panoramic Google Street View update. Have you nothing to hide then?

Data and metadata can be equally menacing in the context of this nothing-to-hide idea. Most times, both types generated by individual and corporate use – just like the historic I am leaving behind of bibliographic references available online to assemble this piece of writing – are "inconsequential, even beneficial". But if they are freely accessible in the hands of security agencies, there's not only

[50] Tudge (2010), p. 19.

[51] Differently, *idem*, pp. 107 ff.

[52] Stylianou (2011), p. 51. Although the author then considers that the technological effect on monitoring might render itself "practically innocuous" because, outside these clear violations of privacy which would strongly hold up in court, most individual information collected is just "lost in translation" among the numerous frames caught with other people's data.

the downside of having an undesirable someone snooping around our personal stuff. There's also the possibility that the kind of associations they make are wrong or false. They are not immune to misidentification, corruption, or fraud. As Lyon puts it, connecting fragments of unconnected data is often "based on stereotypical assumptions about people from particular backgrounds [and] may create apparently incriminating profiles that are readily seized upon by those taught to think that citizens-in-general may be masquerading as terrorists. People with no criminal record, who have done no wrong and have nothing to hide may yet have much to fear"[53].

Besides qualitatively violating several fundamental rights, the argument fails to convince also for a sort of quantitative defect: its multiplication requirement. The number of times one could hypothetically end up having to prove his "innocence", *i.e.*, that he had nothing *bad*, legally wrong, to hide from public view or law enforcement, makes the argument quite harmful in practice.

Every time an individual faces any monitoring apparatus, he must display part of his identity, of himself, to others. Based on the argument, one could go as far as to say that, provided he has nothing embarrassing to tell the authorities (or private companies!), then he should submit and be scrutinized repeatedly, every time they pleased, with no right to keep his affairs secret or private. Otherwise, he could immediately be suspect of trying to hide something criminal, even if – and there would be no room for contradictory, in a very much *kafkian* logic – he was only attempting to conceal his own assemblage of the self from prying eyes. Truly, agreeing with the argument could lead to a "slippery slope" of allowing for the multiplication[54] of monitoring systems with a wider and denser capacity of surveillance and barely any limits. What counter-argument could then be used to deter monitoring? If law-abiding citizens have nothing to hide, they won't mind intrusion and so there are no restrictions, namely of checks and balances, to surveillance.

One could argue that this is nothing short to hypothetical. That this robust surveillance attitude doesn't happen in democracy and that arguing based on abstract ever-present monitoring systems is absurd. Democracies have, nonetheless, been smothered for less.

[53] Lyon (2015), pp. 75-76.

[54] "Institutionalization" of data use multiplies the effects of gathering information, especially when there's an almost "professionalization" of the searching and collecting methods. See Rule (2007), p. 195.

In the private sector we trust

The state is no longer the sole owner of surveillance mechanisms. It has dominion only over regulations on the use and licensing. Although governments are becoming more aware of their citizens' personal data, the private sector is now the dominant force in collection. Public services rely on identification, CCTV, and specific info contained in health or financial records and they produce an important bulk of material on citizens. But private companies usually access, retain, and process much more, with modern computing permitting the circulation of data at a massive level[55].

Consumers are usually willing to give far more information online than on physical formats. Some businesses approach their customers by asking for data optionally and even provide cards for future purchases. Most, however, either create a commercial profile on their systems or prefer the client to follow a specific link to their websites to register there. Individuals enroll to access the benefits the company seems to "altruistically" provide them[56]. The amount of personal data quickly becomes nothing more than a stone in the shoe of having a profile and thus enjoying the new "personal relation" with the company. Like it was a sort of status that made that client special, different. And, in the end, who will suspect of the mailshotted questionnaire with a chance to win an appealing prize provided you freely disclose all manner of personal data?

Public services, on the other hand, seldom relinquish a physical act that gives a degree of solemnity, public certainty, and legal bond to the interaction between the citizen and the administration. It enables the latter to know who is the former, or his legal representative, and better guarantees that someone is not pretending to be someone else while interacting with the executive. In fact, an important difference between digital and physical interactions, transposable to the private *vs* public relations, derives from the distinction between privacy[57] and anonymity. Unlike individuals feel, the private sector seldom cares about exactly who sits on the terminal end of their network or joins their freely-accessible loyalty services. While e-government rests on information about an individual because of who he is, the anonymity of commercial requests is less to do "about the person per se,

[55] Angwin (2014), p. 30.

[56] As Stylianou (2011), p. 51, argues, "privacy is likely overestimated, often because we fail to put the loss of privacy in perspective thereby exaggerating the potential – but rarely realizable – dangers, and that even when the dangers are real, people are often willing to compromise their privacy for the benefits a given technology has to offer".

[57] The different definitions and debates around the concept of privacy will not be discussed here. For the purposes of this text, it was adopted the notion of "informational privacy", *i.e.*, the extent to which someone can control the disclosure of his personal data. It involves the right to be free from prying eyes and the actual control over the intelligence once it reaches third parties, according to Lloyd (2011), p. 11.

but their behavioural patterns…for wider profiling purposes"[58]. Private entities set commercial reports to profit from numbers. They look at personality traces in an economics perspective, not a political one. Their "interest" is not aiming at either friendliness or ensuring citizens pay their debts. It's purposely-driven in a blank and massive way that leads to consumption of their products.

Surveillance defines aspects of the interactions between people; also between the state and its citizens. Nayar says that "surveillance is a form of *governance* not only by the state but by non-state actors as well"[59]. The problem, nonetheless, is that we trust (more) private actors because we usually don't feel their governing pressure. And also because we imagine the readers of our uploaded contents to be as distant as the internet itself, often leading us to forget basic rules of behavior and that an "offline comeback" might be a serious impending threat[60].

Unlike when it comes to public surveillance, a common user won't fully realize or mind most private apparatuses. Knowing the surfing whereabouts, the number of clicks, the time spent on webpages, or with the mouse pointer over certain contents is somehow different from being monitored by police cameras on poles. Nevertheless, the personal consequences can be just as serious. Insurance companies can snoop around for undisclosed details of personal life, universities and corporations can verify the background and current activities of staff and students, and private secret services' job are made much easier as they can outline a profile with just a few clicks. On the other hand, while some online tools permit users to delete or edit information provided, thus making them have a certain degree of control, others are quite reticent to do it. Google, for instance, has been under the spotlight for hanging on to (too much) information[61]. Although sometimes the record left behind linking IP addresses and searched keywords can have positive outcomes[62], having a permanent history of your online activities in the hands of usually unaccountable private corporations should have a "chilling effect", even if you are not planning to do anything unlawful.

Citizens should realize that everyday monitoring by private parties means that ordinary people – not secret services or accountable public officials; or, at least, not only – are checking, gathering, processing, and storing their personal data with barely any limits. Adding this to privacy options that can make your e-mail contents searchable for meaningful advertising and your cell phone a

[58] *Idem*, p. 6.

[59] Nayar (2015), p. 3.

[60] Tudge (2010), p. 16.

[61] Court of Justice of the European Union (CJEU) ruling C131/12, *Google Spain and Google*, 13 May 2014.

[62] See the criminal case illustrated in Tudge (2010), p. 18.

permanent GPS tracker[63], makes trusting the private sector something like mice trusting cats. Not to speak of the fact that almost any website is susceptible of hacking[64].

When it comes to online contracts, for instance, the fact that they are "shielded" by legal guarantees, even if we don't read them, gives the appearance of safety and security concerning our data and how it will be handled. But the fact remains that private monitoring can be just as systematic and intrusive as public monitoring. The thickening of data retrieved by corporations can reflect legal demands that allow and "encourage" for the piling of clients' personal information. For instance, years ago telephone companies used to collect only basic metadata – things like the duration of calls, when they took place, and the location of the connecting devices. Nowadays, phone invoices detail everything about our conversations, except the content. Businesses are required to supply all this intelligence so that clients know what exactly they're paying for and can control their usage figures[65]. This way, companies are not only encouraged but obliged to have enormous databases and often their contracts with third-parties (sub-contractors) to manage the data severely jeopardize privacy. As Lord Hoffmann put it, "the right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat"[66].

Acceptance towards self-surveillance (through exposing our personal lives on social networks) and informal surveillance, *i.e.*, by creating commercial profiles, add up to state surveillance in the filling of the gaps of information. It's important to keep in mind that a good deal of the intelligence states gather comes from private agents in the marketplace, usually from purchasing goods and asking for an invoice. We know there is an "invisible chain" connecting private networks and public databases but we don't link any of them to the idea of surveillance, thus trusting the non-state sector when it obviously depends, relies, and passes information to governments. And while most people worry about their information ending up in public records, they forget that most private CCTV operators are not properly scrutinized, for instance, to comply with the right of access to the data[67].

The phenomenon of decentralization of surveillance through public and private forms of observation[68] can lead to a culture of suspicion but also to a culture

[63] Tudge (2010), p. 18.

[64] *Idem*, p. 17, gives the example of the 2005 hacking of Facebook where two students of the Massachusetts Institute of Technology downloaded data from 70,000 profiles for a research project.

[65] Lloyd (2011), p. 8.

[66] *Idem*, p. 9.

[67] Berg (2015).

[68] Nayar (2015), p. 4.

of "neighborhood knowledge". Although physical surveillance is as old as society itself[69], we want to know more and more about what other people do, say, think, and even eat – specially those closest to us, the neighbor behind the lace curtains. Talk shows, soap operas, and human interest stories are apparently innocent examples of how individuals know about others, either real or fictitious. But this "convergence" generates blurred surveillance, mixing different aims and roles, actors, and processes[70].

One could then ask whether new technologies creeping on most aspects of modern life can damage the quality of our consent to this way of things. Consent here will be used in a broad fashion, ranging from the general consent to be part of the social contract to more limited ways, such as acceptance, implicit or express, to engage in legal contracts online. The traditional idea of consent to contract rests on the assumption that the interested parties know the full scope of the bonds – they are not only aware of the new legal norms befalling on their particular relations but they usually are part of the process of drafting such rules, which gives a degree of commitment to the contract *per se* and, specifically, to how they shall enforce it. And even if they haven't been part in the making, they must, at least, have all the necessary data to accept and comply with the rules that apply. This happens in obviously different ways, as alluded, if one's talking about formal contracts or in the context of the so-called social contract.

By trusting the need to be surveilled and accepting monitoring from different entities through contracting, we pile up "moments of consent" that end up making us agree, *i.e.*, consent, to be surveilled in almost all moments of our digital lives. In the end, they come to change the social contract – that invisible agreement that makes us irresistibly part of the political society – by adding extra layers of "tiny" self-surveillance here and there.

Are we consenting to be surveilled?

Some literature sees surveillance as a mechanism for social sorting[71] but I agree with Nayar when he considers it to be more of a "phenomenological element that informs, influences and inflects even our interiority"[72]. Surveillance is not necessarily a bad thing *per se*[73] and it appears to be embedded in our citizenship, like part of the ever-present and ever-renewed social contract of

[69] Lloyd (2011), p. 15.

[70] Nayar (2015), p. 4.

[71] For example, Goos, *et al*. (2015), pp. 51 ff.

[72] Nayar (2015), p. 2.

[73] Angwin (2014), p. 37.

modern times. In an unsettling perspective, we could redo René Descartes' most known quote to "I am surveilled therefore I am"[74].

Users' consent[75] is at the core of attempts from the judiciary[76] to shield privacy and keep high standards of data protection regarding personal information. Like most social interactions in life, accessing virtual communities or agreeing to contracting online depends on consent. But in the e-space, the quality of consent can be tainted. We are witnessing that more and more individuals are not aware that their personal information is being collected or, at least, how it will be used[77]. This way, they have no opportunity to consent or withhold consent in a meaningful and timely manner. Consent is thus a key principle of any data protection regulation but how to "solidify" that consent has been a debatable matter, specially *viz.* the global dissemination of data by online tools that no data subject can ever fully grasp, let alone control[78].

The "massification" of contractual operations (joining a social network, shipping orders, etc.), particularly undertaken by younger generations, can begin to explain how little time we devote to read online (legal) documents. Hardly anyone truly weights the pros and cons of ticking the box as that would amount to reading 20 or more pages of tiny lettering with a profusion of obscure legal terms. Why bother when you can just scroll down or skip ahead and click on the box next to the "I understand the terms and conditions" phrase? Is not like anyone reads it. And it's not like anyone is watching over your shoulder and making a disapproving nod at you. Right?

[74] Nayar (2015), p. 2.

[75] A trace of the principle of collection in data privacy regulations. See, *inter alia*, Article 7 of the Organization for Economic Co-operation and Development Guidelines on the protection of privacy and transborder flows of personal data, Doc. C(80)58/FINAL, adopted on 23 September 1980, which reads that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject". Also, Greenleaf (2013), p. 237.

[76] For instance, in the judgments on the merits delivered by the Grand Chamber of the European Court of Human Rights *Bărbulescu vs Romania*, no. 61496/08, 5 September 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy vs Finland*, no. 931/13, 27 June 2017, *Roman Zakharov vs Russia*, no. 47143/06, 4 December 2015; the case law of the CJEU C-73/16, *Peter Puškár vs Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*, 27 September 2017, C-203/15 and C-698/15, *Tele2 Sverige AB vs Post- och telestyrelsen and Secretary of State for the Home Department vs Tom Watson and Others*, 21 December 2016, C-582/14, *Patrick Breyer vs Bundesrepublik Deutschland*, 19 October 2016, C-362/14, *Maximillian Schrems vs Data Protection Commissioner*, 6 October 2015, C-293/12 and C-594/12, *Digital Rights Ireland Ltd vs Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, C-524/09, *Ville de Lyon vs Caisse des dépôts et consignations*, 22 December 2010; or the ruling of the General Court of the European Union T-343/13, *CN vs European Parliament*, 3 December 2015.

[77] See the balance between benefits and harms in Edwards (2013), pp. 315 ff.

[78] Tudge (2010), p. 15.

The smooth way in which one can skip ahead of reading the details of e-contracts should be worrying in terms of their legal validity, in terms of the consent given and the strength of acceptance of all the terms, perks, downsides, and conditions of engaging into contracts in the virtual milieu. Some websites make sure that, at least, the contract is viewed in full by blocking the following steps until the user has reached the bottommost line. But does this suffice? These are scenarios where the pressure of signature, that is, of having a pack of pages with a contract in one's hands and having to sign it in the end (and perhaps also rubricating each of the previous pages), is, for all its worth, absent.

Let's take a small step back and breathe in. Surveillance is not necessarily opposed to any sentiment of privacy. They are flexible concepts and, just like most legal interests and rights, they have ambiguous borders. In some respects, it could be said that the degree of privacy is still maintained when the personal data provided is accessible only to a select group of people with proper access codes. There are policies that entities can implement to restrict the viewers of databases, like those based on hierarchy. The concern deepens, however, when individuals are driven to hand out information on a regular basis and there are little or no guarantees of who will handle it. They can ask for privacy on a general basis but, from an external onlooker, it would seem most people do "little to protect themselves"[79]. Thousands of individuals join communities that share intelligence every day, not to mention what goes on at the retail level. As Tudge put it, hyper-exhibitionism online has just taken a step further, from glamour to the banal[80]. And for marketing purposes, it's very hard to make sure there is only a few people with access rights that read the data. A customer's file can go back and forth between the several departments of a corporation, be copied multiple times, processed in several computers, and analyzed by many different white collars. And we are not talking about secret services or top-level state departments. We're talking about normal, private, businesses with normal, private, human resources policies.

There is not yet a new balance, both in the mindsets as well as in legal writing, in terms of new meanings for data protection, privacy, secrecy, or consent in current times. The US are more "advanced" in terms of surveillance schemes, governmental or corporate, while Europe still struggles – perhaps positively – with keeping the core of human and fundamental rights safe from prying eyes. But in both sides of the Atlantic, in an almost anecdotal way, peeping through the keyhole of a bathroom is instinctively perceived as a privacy violation, while being under the radar of inter-connected surveillance mechanisms in a mall or

[79] Lloyd (2011), p. 11.

[80] Tudge (2010), p. 15.

an airport, ranging from CCTV to biometrics, is…well, not. Airport facilities are, in fact, the "epitome of surveillance-oriented" societies[81], denying the anonymity of passengers while increasing the identification of travelers in a *quasi*-direct proportion from the entrance to the boarding gate. They, sometimes literately, strip you down[82]. There operate several entities with different agendas and monitoring devices, from the private sector to governmental immigration bureaus, in a sort of "ecosystem of integrated surveillance". As Ogura argues, technology permits surveillance of the individual to go well beyond the confined space of the airport as the processing of data in the electronic microchips of passports and of visual and sound material from CTTV and cooperative mechanisms is usually not done exclusively through data systems located inside its physical space. Data can even travel somewhere outside the host country with little technical restriction. In such an "oppressive" context, it seems "we have no other choice but to sacrifice our privacy rights"[83] – which renders any notion of individual consent from the surveilled parties irrelevant. And we're not even talking about online users in these examples.

Irion makes an interesting argument when stating that a handicap in finding this new balance is that constitutional and legal checks and balances to counter unlimited surveillance have developed in the framework of targeted surveillance. Safeguards that are thus appropriate to direct and limited monitoring performed with strict oversight and usually in the context of criminal investigations are naturally insufficient to refrain mass surveillance. However, there has been no significant legal adjustment in many countries to create or update (or upgrade, truth be told) such arrangements to mass surveillance. And the fact is that "preemptive and systemic surveillance exceeds qualitatively and quantitatively the situation of targeted surveillance"[84] by far.

A U-turn where strong and traditional privacy and data protection concerns prevent the flow of data between legal orders and deter private and public access to citizens' personal information does not seem a likely scenario. Commerce depends on trade, namely trade of information of the people involved in the transactions. It's a form of building trust. A form of getting to know the other side, especially *viz.* the fact that most companies display their institutional and organizational features to the public on their webpages but don't know much about the buyers of their products when they first come to shop. But it's arguably a form of using knowledge to make profit.

[81] Ogura (2006), p. 281.

[82] See the case studies on airport and CCTV present in Neyland (2009), pp. 30 ff.

[83] Ogura (2006), p. 281.

[84] Irion (2015), p. 82.

Surveillance is bound to evolve with the concept of society in Western democracies. Nayar is sharp when instigating us to "start thinking about surveillance not simply as technological mechanisms of control…but as a cultural phenomenon"[85]. However, the development of this "phenomenon" should be halted when "distrust becomes normalized, repackaged and marketed as a proper (and profitable) state of mind"[86]. CCTV, above all, empowers the hierarchical division of power in the system of those who watch and those who are watched and its fast development is now capable of turning an anonymous face, a John Doe, into a concrete individual in a matter of hours, or much less. From facial recognition to tax revenues, the interoperability of databases enables watchers with a sufficient access level to quickly grasp indexes of personal and sensitive data faster than ever before. What does this imply in terms of the "anonymous public"? What does it do the idea of preserving one's personal data, other than our own face, among the throngs of fellow by passers? Also, it's interesting to dwell on the possibility of local communities accepting or rejecting these intruders – is there such an option at all?

Although many consider surveillance to enable a better, safer, society, most people are powerless to say whether they would prefer to be surveilled or not. This becomes a serious concern when most surveillance dragnets go beyond our previous notions of traditional surveillance, being "suspicionless, computerized, impersonal, and vast in scope"[87]. They create a sort of "shadow surveillance", which could potentially turn modern, even robust, democracies into police states. There is a real concern that a slippery slope may appear when these powerful data gathering and mining tools are used for increasingly pettier needs until societies are smothered under a "veil" of constant surveillance and are thus unable to (re)organize themselves without surveillance gears.

For Nayar, a line can be drawn between those who are surveilled regardless of their will (like commuters on public transportation) and those who opt to be surveilled by adhering to self-surveilling mechanisms, such as social networks. As the author says, a line between compulsory and voluntary sharing of data, which apparently leads to a stark difference in terms of ontological data subjects[88]. But is it *that* simple?

[85] Nayar (2015), p. 5.

[86] Tudge (2010), p. 159.

[87] Angwin (2014), p. 37.

[88] Nayar (2015), p. 31.

The problem of consent[89] has many nuances and it might not be entirely accurate simply to say that people can choose not to have an account on a social network or that they could refuse adhere to loyalty cards. Even setting aside the leakage effect, *i.e.*, the passing of data to third-parties (the core of cookies' debates) – and which are often outside the knowledge and control of the data subject –, the fact is that these so-called voluntary transfers of personal data may not be that *voluntary*, in a way. In some less-surveilled cities, where surveillance isn't almost impossible to avoid, one could say that the individual could diminish his exposure by taking some "precautions", like driving a personal vehicle instead of taking a public transport, avoiding areas where he knows there is a CCTV system installed, and so on. This way, compulsory surveillance would look like voluntary surveillance, in some situations, and the individual would be shielded against certain prying eyes. However, wouldn't this end up by being an erratic behavior, defeating basic common sense or any sustainable way of living? It would make the life of the individual far more complicated, impossible perhaps in the long run, not least for economic reasons.

In a similar fashion, avoiding the perks of loyalty cards, frequent flyer miles, or, in less obvious manners, having an account on Facebook[90], could lower the quality of life of individuals. These are advantages of modern life that come with a price. Advantages that most people can live without – at least some people, for now – but that are becoming normal, everyday, stuff and rapidly looking less and less like advantages or whims. This "voluntary consent" to be surveilled in such cases might not be so voluntary after all because the services and goods provided are more and more part of what it means to live in the present times. And this is why even those fully aware of the potential monitoring shadow of certain (online) activities and of the consequent social control, seldom modify their behavior. Those services are embedded into the fabric of our current social existence, transforming themselves, sooner or later, into compulsory facilities.

In fact, "as well as being a commodity in its own right, data is the motor and fuel which drives the information society"[91]. Already having a loyalty card in a supermarket that offers discounts in future purchases hardly seems an advantage most people can (easily) live without. What about travelling? For some people, it's a necessity. For others, a commodity. It's a borderline scenario where voluntary and mandatory consent are quite hard to untangle – and one should

[89] Unlike argued by Rule (2007), p. 170, people often choose and thus consent to provide personal data and have their privacy violated, in several different ways. The nuances of the concept focus precisely on the type of consent for each type of data collection. People have been relinquishing – and the issue lies at the heart of their knowledge to consent – to secrecy of their data to get something in return, which depends on the context, from the direct scale of user-social network to the indirect of public-CCTV, for instance.

[90] All examples present in Nayar (2015), p. 31.

[91] Lloyd (2011), p. 15.

not only consider "surveillance-overloaded" airports as there are CCTV and other forms of surveillance in most bus and train stations. And what about when consent is virtually inexistent, like when a satellite photographs you to update an online map? Are you tacitly consenting when you're…walking outside?

Removing those "perks" is certainly not that easy or straightforward for most people and in most sectors of economic activity. New economic sectors beyond the traditional three-party division depend heavily on modern technologies. If the tertiary sector, composed of service-based activities, already relies on some surveillance-based equipment (computers above all), the quaternary and the quinary exist because there are supporting technologies. The former consists on knowledge-based activities and the latter on intellectually-based activities at a macro level. The quaternary is concerned with the "non-physical" organization of the society, comprising government, research, cultural programs, IT itself – like services providing information, such as computing, ICT, or consultancy –, and education. The fifth level is similar to this one but only bridges top (senior) management levels. Both are developments of the tertiary group that have sprung from the computerizing of society and the inherent exchange of data that keeps it running.

Modern society, particularly in Western countries, comes indeed with a surveillance "price tag". It's like a parasite latching onto modern technologies and growing fatter as they themselves expand. If you think about it, computers didn't have cameras in their beginnings in the 1960s. Nonetheless, today they are one of the prime tools for checking on an individual. Research, development, and widespread use have followed the path of information sharing because that's the funny logic of using technologies – to enable us to get in contact with each other, not physically but through a parallel world. It's only natural that we feel slightly bothered by having someone snooping over our shoulder 24/7. But, in the end of the day, we are the ones who have invited him, aren't we? As modern societies are computerized societies, the technological advances that make our lives easier should not be perceived as something to be purged – it's even hard to picture a 21st century day with no technology apart from some small communities that have somehow resisted the passing of time in remote areas of the world. And we can instantly detect how living without it would make us feel uncomfortable, to say the least. Technological leaps are advantages and they are necessary and an integrated part of our idea of society, of living together in a community.

So, the difference between the "genuinely disempowered and placed under surveillance and those who *opt*"[92] is a more complex issue than meets the eye.

[92] Nayar (2015), p. 31.

The internet supports most of the daily activities of steadfastly increasing fractions of the global population[93]. In fact, technological communications permeate literally every aspect of modern, contemporary, life because they satisfy "human's need to socialize and connect with others"[94]. And online activities also affect offline behaviors[95]. Deep down, our consent derives from the safety and sense of protection that monitoring provides – from the legislator down to your regular by passer. And anything that makes us feel secure, that broadly advertises serving to catch the "bad guys", is usually seen as a good thing. The more we believe CCTV should be used to monitor our movements and thus deter crime[96], the more surveillance will be embedded in our social selves. We surveil and are surveilled – after all, it's for everyone's benefit. But we share information with corporations not because there is a monitoring system in place. We do not answer questionnaires because we really want someone to know what we bought and when. We consent to those "little" trade-offs of having our personal information depart our private sphere because we have come to believe it's all needed, that it should be like that, perhaps even for some sort of greater good. Nevertheless, sometimes this preventive surveillance[97] is based on little evidence that the balance of interests at play is adequate, necessary, and proportional.

Public ignorance regarding the full scope of surveillance[98] (and to whether there is someone actually sitting on the other side of the prying eye) or simply our willingness to obey the rules can lead to the curious effect of public acceptance, consent, provoking good inner feelings. When we grow aware of our consent to surveil and be surveilled (like "accepting" to go through biometric identification), and we start playing along with the system, we often let our vulnerability be transformed into compliance, tolerance, and adaptation. And then we feel law-abiding citizens, accepting surveillance and our "duties" under someone else's gaze. We let ourselves be engulfed by the culture of surveillance and then

[93] Thelwall (2013), p. 69.

[94] Irion (2015), p. 79.

[95] Thelwall (2013), p. 70. Also, in general, Nardi (2010).

[96] Usually based on the fallacious idea of the "rational offender". For Norris (2012), p. 256, this consists on the assumption that non-offenders, are "aware of the presence of the cameras…Second…that, even if the offender is aware of the cameras, [he has] factored them in to a rational calculation…Third…that, while the rational offender is deterred, the same offender appears not rational enough merely to commit the crime in a different place, or choose to commit a different type of crime less susceptible to camera surveillance. Finally, it assumes that, if the offender is aware of the cameras, [he] will be deterred…[Nonetheless, research] with street robbers, burglars, shop thieves and card fraudsters has revealed that few indicated that the presence of cameras made any difference as to whether they would commit a crime or not". Is it then that only the law-abiding fear CCTV?

[97] Nayar (2015), p. 7.

[98] Tudge (2010), p. 85.

there is little more than "*fashion* ourselves as surveilled citizens…performing in particular ways in front of the camera"[99].

The presence of surveillance mechanisms tends to modify our way of interacting. It can produce no visible effects on human behavior but it usually does. At least, from the moment the surveilled realize they're being surveilled. As Nayar argues, IT changes not only how we interact among ourselves but the permanence of a surveillance gear in a place, specially indoors[100], changes how we come to deal with it, not the least on the long run. Even if we do not become exemplar citizens like suggested above, we get accustomed to do things in a way, perhaps even turning us into a better version of ourselves under that familiar gaze to which we might get used to. In fact, it's very hard to effectively reject surveillance once the public as a body accepts to be under the technical prying eye.

Surveillance is needed, particularly in times of insecurity. That should not be realistically denied. But too much surveillance can lead to too much suspicion and boost bad sentiments towards living in community. It can trigger emotions and anxiety that lead people to become less rational in their social interactions. The "culture of insecurity", especially when it is exacerbated before the real threats and dangers of the modern world, makes vulnerable subjects out of users, nationals, neighbors, and friends. And then surveillance is used as a token for freedom – the common-place of a "small" price to pay against insecurity, vulnerability[101], and fear.

The main consequential problem with this culture is its multiplying effect. A culture of surveillance tends to generate "culturally-surveilled" subjects, that is, people who don't strive or see the need to question the surveillance mechanisms – silent consenters. Some simply won't care and others will actively instigate it. All perpetuate this culture, the latter perhaps even taking a step further in the subtle oppression. Not only a top-down oppression but a worst kind: an oppression from all sides. Even from within, from ourselves, the data subjects. This way, cameras will remain in their poles and, sooner or later, more will join them. Perhaps cameras won't even be our major concern but instead our own attitude towards surveillance and towards others.

Given this scenario, it could be argued that surveillance becomes a "culturally accepted and culturally legible process"[102]. In the end, a culture of insecurity leads to a culture of surveillance, or surveillance-oriented[103]. And so forth: we

[99] Nayar (2015), p. 33.

[100] For a comparison between different surveillance tests, both in and outside buildings, see Angwin (2014), pp. 45-46.

[101] Nayar (2015), p. 5.

[102] *Idem*, p. 6.

[103] Ogura (2006), p. 280.

truly become surveilled citizens[104]. Plus, we want to belong to the many offers of society, to adhere to consumption models, to be part of travelling plans. And there is nothing wrong about the plentiful offers modern society has to provide, so long as they can be understood and apprehended rationally. As this culture of belonging[105] comes with precautionary, often preemptive, surveillance, we, as individuals and as citizens, should be aware of becoming surveilled (political) animals by our own consent. A consent that can either have thin legal grounds and be recklessly exercised or that can be refrained, tamed, educated, and nurtured. It's not necessarily the "fault" of others the immense surveillance we are embedded in – consent and accountability should be the base for "harvesting personal information", translated into purpose limitation, non-disclosure policies, and a controlled retention rationale[106]. A healthy, informed, consent and a surveillance attitude balanced by reasonable security and privacy concerns (which are both democratic interests)[107] are only possible with a shared commitment by all relevant parties – citizens, governments, corporations, and (especially) security and intelligence agencies[108] – of checking and balancing each other.

Technologies have evolved to permit surveillance from a distance and to permit the collection of material without the presence of the person, especially when information systems are interoperable, *i.e.*, able to communicate in a quick and effective way without loss or damage of data. A consented surveillance culture

[104] Particularly seen as groups and less as random individuals. It's interesting the idea of change in the *ratione personae* paradigm with the new technologies of mass surveillance in Sloot (2017), p. 75.

[105] Nayar (2015), p. 8.

[106] Lyon (2001), p. 129.

[107] Lyon (2015), pp. 98 ff. Although questioning the consistency of mass surveillance and democracy further in pp. 107 ff. The author also stresses that not many really see mass surveillance as a peril to democracy, facing its growth "more as necessary than negative". As long as there are thousands of bureaucrats and systems' analysts sitting in desks at computer terminals managing someone else's data and metadata, there might be a risk of a sort of "corporate Holocaust", an updated and perhaps much more terrifying version of Hannah Arendt's banality of evil. And it's true that security can trump politics when fear settles in. Nonetheless, as he comes to recognize as well, "in some respects democracy depends on surveillance".

[108] Data collectors must change their "default position" (in a social-organisational sense, not a technical one) from deciding to collect to trying not to collect information, in the words of Brown & Korff (2010), p. 12. Both governmental and private policies should pay lip service to the principle of no surveillance "without meaningful individual consent or legislative authorization" [Rule (2007), pp. 195-196]. As the author continues, "taking privacy seriously…would amount to a revolutionary overthrow of practices now prevailing in the United States, and to a lesser degree elsewhere [and] entail that any commercialization of personal data, either from government files or private-sector records, would require active assent from the individual concerned. In the jargon of privacy-watchers, 'opt in' would be the rule". And perhaps this can be taken beyond commerce. In fact, the author's definition of commerce – "activities aimed at creating value for institutional decision making on the people concerned" – seems to accommodate areas where there is no actual commercialization but where, nonetheless, personal data is used in other meaningful ways, such as state surveillance. Although an important shift in action but also in mentality, this "individual veto power" is crucial to the sustainable development of surveillance practices and to raise awareness to the full implications of consent. See also, Greenleaf (2013), p. 247.

appears to be one of the prices of cosmopolitanism, of globalization. However, just like any (social) phenomenon, it should develop in a sustainable way. This is a complicated proposal as many factors influence the creation and spread of surveillance apparatuses. But if advocates and political agents focus policy and law-making on consent and accountability as an inseparable pair of the surveillance framework, any "free ride" (or free fall) monitoring can surely be slowed down and be made sustainable.

Concluding remarks

Unlike what happens in some papers, it is hardly conceivable a one-size-fits-all solution here for what can be the sustainable evolution of mass surveillance in times to come. Nowadays, there are different degrees of integration of peoples and societies in the electronic world. Sooner or later, however, all communities will be online. This moment will mark an unparalleled cut with the time before computational technologies. Their lives and their culture will change. Culture is the result of human interactions, the product of human activity, rites, and traditions. Technological development is too powerful, too useful, and too helpful to be ignored in the design of human societies and their respective cultures. Perhaps even in the design of what it means to be human in the contemporary world of today and tomorrow.

What must be borne in mind is that surveillance is a political and social choice. Big data collection and general monitoring practices that reverse the order of police suspicion and gathering of evidence[109] to a system of extracting every kind of intelligence and making everyone a person of interest first is also a choice. Surveillance[110] is not an inevitability or a disgrace that cannot be controlled, tamed, or even made transparent and accountable. It is true that some "surveillance systems have a life of their own – they creep into new areas, absorb more powers. The danger is that we are creating a world built on distrust in which there will be literally no escape from those who are watching us"[111] – one of the many, quite real, risks ITs present[112]. But even if it becomes embedded into how we perceive the world from a young age and if we no longer can live without

[109] Lyon (2015), p. 77.

[110] Or "dataveillance". See curious references in some literature, namely Lyon (2015), p. 76; Goos, *et al*. (2015), p. 72, mentioning the coinage of the term by Roger Clarke in the 1980s; Raab (2015), pp. 260 ff; or Fussey & Coaffee (2012), p. 207.

[111] Tudge (2010), p. 146.

[112] For an account of nine risks (nightmares) that fictional literature has presented in the last century to human rights, see Sartor (2013), pp. 14 ff.

these silent prying eyes, surveillance operations – regardless of their form, size, or shape (but particularly within large-scale programs) – can, should, and must depend on clear and informative processes; with the possibility of making the data accessible; and with watchers legally accountable, both internally and externally, in due processes and through reasonable means in the hands of the surveilled individuals or their representatives. It is important to come back to ground notions, such as secrecy, discretionary powers, or security exceptions, and to re-think them through a careful balance of the interests at play. Especially when we can have glimpses of grimmer times and envisage a future of almost absolute monitoring – we are not treading (totally)[113] in the dark here. We know where and how to go forward and so we only need to be intelligent about it.

A "free riding" surveillance attitude, either from governmental agencies or private parties, should be questioned at the local, regional, national, and even inter-state (international) level. Opinions will always diverge on this matter but the fact is that surveillance is bound to grow and expand with the evolution of technology. If this fact is a given – and it is, be sure of that – legislators and governments must tackle the issue keeping up with times and not pretending to deter the healthy development of technology.

Law-making will never keep pace with technological progress or surveillance techniques[114], especially while they are still perceived in a traditional and targeted way. As such, this must be approached by tying the legitimacy of electronic surveillance to accountability of the monitoring parties[115]. In the surveillance discourse, the preference should be for: *i*) quantitative and qualitative limitations of surveilling mechanisms; *ii*) a constant reminder to citizens of vigilance demands in any given area; *iii*) informing individuals when their data is retrieved and granting them access to the collected information under serious penalties; *iv*) transparency of all processes – in itself a "prerequisite of accountability"[116]; *v*) legal and constitutional justification of the intrusion tied to *de iure* and *de facto* liability of the watchers; and *vi*) preemptive scrutiny by independent boards. This last criterion is nothing extraordinary and would involve very similar requirements to independent regulatory agencies, such as those operating in the banking, energy, and environmental sectors.

All these demands are opposed to currently "tolerated" situations of indiscriminate surveillance, unjustified vigilance, staged militant political activism,

[113] Sartor (2013), p. 19.

[114] For a careful assessment of the European legal standards in technological development, with a special focus on the surveillance programs by the British Government Communications Headquarters or the NSA, see Bigo, *et al*. (2013).

[115] Irion (2015), p. 82.

[116] *Idem*, p. 83.

or disproportionate scrutinizing under misplaced counter-terrorism and fight against crime. As Irion put it, the "knowledge about the mere existence of blanket surveillance schemes is not equally as compromising as it would be for targeted actions. To the contrary, democratic societies should rethink the contours of secrecy, because the public sacrifice to national security must be transparent to its constituency"[117]. There are many dangers lurking from covert surveillance programs, particularly the persistence of social and racial ghettos by drafting inaccurate images of the "other"[118].

In the end, states are responsible for surveillance as they set the boundaries for what is permissible[119]. No private or public monitoring should be permitted without public administrations being aware of it. This should extend as far as considering that foreign monitoring through private companies must never be unknown to host governments. And there ought to be legally binding international and regional commitments to the accountability of the parties and surveillance powers, not only political ones. However, as surveillance is part of the idea of (constant) democratic accountability, governments should not be accountable only in electoral moments. No surveillance operation should be (absolutely) covered against public, democratic, and transparent legal scrutiny in due time and by the appropriate agencies. Otherwise, there is a serious risk of erosion of the very democracy it is supposed to defend.

[117] *Idem*, p. 84.

[118] Skoczylis (2017), pp. 119 ff.

[119] An interesting "permissible limitations test" suggested by Scheinin (2013), p. 588, would help maintaining the inner core, or *forum internum*, of the rights to privacy and data protection within the logic of surveillance programs. Although the author is referring to international human rights law, it could easily be mimicked at the regional and national levels.

Bibliography

AAVV, 1992, "Employee stress and health complaints in jobs with and without electronic performance monitoring", *Applied Ergonomics*, vol. 23, number 1, pp. 17-27.

AAVV, 2013, "Mass surveillance of personal data by EU member states and its compatibility with EU law", *CEPS Paper in Liberty and Security in Europe,* issue 61.

AAVV, 2015, "The co-evolution of surveillance technologies and surveillance practices", in *Surveillance in Europe*, David Wright & Reinhard Kreissl (eds.), Routledge, London, pp. 51-100.

AAVV, 2017, "Big data and local performance management. The experience of Kansas City, Missouri", in *Routledge handbook on information technology in government*, Yu-Che Chen & Michael Ahn (eds.), Routledge, New York, pp. 95-107.

Angwin, Julia, 2014, *Dragnet nation. A quest for privacy, security, and freedom in a world of relentless surveillance*, Henry Holt and Company, New York.

Berg, Nate (2015), *What happens when you ask to see CCTV footage?*, in https://www.theguardian.com/cities/2015/sep/22/cctv-cameras-capture--almost-every-move-on-city-streets-what-happens-when-you-ask-to-see--the-footage (29.07.2017).

Brown, Ian & Korff, Douwe (2010), *Final report of the comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, in http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf (13.10.2017).

Chesterman, Simon, 2014, "Terrorism, surveillance and privacy", in *Research handbook on international law and terrorism*, Ben Saul (ed.), Edward Elgar, Cheltenham, pp. 453-469.

Edwards, Lilian, 2013, "Privacy, law, code and social networking sites", in *Research handbook on governance of the internet*, Ian Brown (ed.), Edward Elgar, Cheltenham, pp. 309-352.

Fussey, Pete & Coaffee, Jon, 2012, "Urban spaces of surveillance", in *Routledge handbook of surveillance studies*, Kirstie Ball, Kevin Haggerty & David Lyon (eds.), Routledge, Abingdon, pp. 201-208.

Gordon, Whitson (2011), *How to stop your smartphone from constantly tracking your location*, in https://lifehacker.com/5854315/how-to-stop-your-smartphone-from-tracking-your-every-move (21.08.2017).

Greenleaf, Graham, 2013, "Data protection in a globalised network", in *Research handbook on governance of the internet*, Ian Brown (ed.), Edward Elgar, Cheltenham, pp. 221-254.

Guarda, Paolo, 2009, "The myth of Odin's eye: Privacy vs. knowledge", in *Law and technology: Looking into the future. Selected essays*, AAVV (eds.), European Press Academic Publishing, pp. 243-254.

Irion, Kristina, 2015, "Accountability unchained: Bulk data retention, preemptive surveillance, and transatlantic data protection", in *Privacy in the modern age. The search for solutions*, Marc Rotenberg, Julia Horwitz & Jeremy Scott (eds.), The New Press, New York, pp. 78-92.

Leman-Langlois, Stéphane & Larivière-Bélanger, Gabriel, 2011, "Les modes de contrôle visuel des infrastructures urbaines", in *Sphères de surveillance*, Stéphane Leman-Langlois (ed.), Presses de l'Université de Montréal, Montréal, pp. 157-175.

Lloyd, Ian, 2011, *Information technology law*, 6th ed., Oxford University Press, Oxford.

Lyon, David, 2001, *Surveillance society: Monitoring everyday life*, Open University Press, Buckingham.

—, 2007, *Surveillance studies: An overview*, Polity, Cambridge.

—, 2015, *Surveillance after Snowden*, Polity, Cambridge.

Marx, Gary, 2016, *Windows into the soul. Surveillance and society in an age of high technology*, The University of Chicago Press, Chicago.

Nardi, Bonnie, 2010, *My life as a night elf priest: An anthropological account of World of Warcraft*, University of Michigan Press, Michigan.

Nayar, Pramod, 2015, *Citizenship and identity in the age of surveillance*, Cambridge University Press, Delhi.

Neyland, Daniel, 2009, "Mundane terror and the threat of everyday objects", in *Technologies of insecurity: The surveillance of everyday life*, Katja Aas, Helene Gundhus & Heidi Lomeli (eds.), Routledge-Cavendish, Abingdon, pp. 21-41.

Norris, Clive, 2012, "The success of failure. Accounting for the global growth of CCTV", in *Routledge handbook of surveillance studies*, Kirstie Ball, Kevin Haggerty & David Lyon (eds.), Routledge, Abingdon, pp. 251-258.

Ogura, Toshimaru, 2006, "Electronic government and surveillance-oriented society", in *Theorizing surveillance. The panopticon and beyond*, David Lyon (ed.), Willan Publishing, Devon, pp. 270-295.

Raab, Charles, 2015, "Effects of surveillance on civil liberties and fundamental rights in Europe", *Surveillance in Europe*, David Wright & Reinhard Kreissl (eds.), Routledge, London, pp. 259-318.

Rengel, Alexandra, 2013, *Privacy in the 21st century*, Martinus Nijhoff Publishers, Leiden.

Rule, James, 2007, *Privacy in peril*, Oxford University Press, Oxford.

Sartor, Giovanni, 2013, "Human rights in the information society: Utopias, dystopias and human values", in *New technologies and human rights: Challenges to regulation*, AAVV (eds.), Ashgate, Farnham, pp. 11-26.

Scheinin, Martin, 2013, "Counter-terrorism and human rights", in *Routledge handbook of international human rights law*, Scott Sheeran & Nigel Rodley (eds.), Routledge, New York, pp. 581-595.

Skoczylis, Joshua, 2017, "Counterterrorism and society: The contradiction of the surveillance state – Understanding the relationship among communities, state authorities, and society", in *The Palgrave handbook of global counterterrorism policy*, AAVV (eds.), Palgrave Macmillan, London, pp. 117-134.

Sloot, Bart, 2017, *Privacy as virtue: Moving beyond the individual in the age of big data*, Intersentia, Cambridge.

Solove, Daniel, 2013, *Nothing to hide. The false tradeoff between privacy and security*, Yale University Press, New Haven.

Stylianou, Kostantinos, 2011, "Hasta la vista privacy, or how technology terminated privacy", *Personal data privacy and protection in a surveillance era: Technologies and practices*, Christina Akrivopoulou & Athanasios Psygkas (eds.), Information Science Reference, Hershey, pp. 44-57.

Taylor, Emmeline, 2012, "The rise of the surveillance school", in *Routledge handbook of surveillance studies*, Kirstie Ball, Kevin Haggerty & David Lyon (eds.), Routledge, Abingdon, pp. 225-231.

Thelwall, Mike, 2013, "Society on the web", in *The Oxford handbook of internet studies*, William Dutton (ed.), Oxford University Press, Oxford, pp. 69-85.

Trottier, Daniel, 2012, *Social media as surveillance: Rethinking visibility in a converging world*, Ashgate, Farnham.

Tudge, Robin, 2010, *The no-nonsense guide to global surveillance*, New Internationalist, Oxford.

World Atlas (2017), *The most spied upon cities in the world*, in http://www.worldatlas.com/articles/most-spied-on-cities-in-the-world.html (21.08.2017).