

Ivana Stepanović\*, MA

## MODERN TECHNOLOGY AND CHALLENGES TO PROTECTION OF THE RIGHT TO PRIVACY

*The right to privacy is a fundamental human right and can be categorised as a first generation human right. However, it is one of the most controversial human rights due to the fact that it is not properly defined. The development of technology has changed our understanding of privacy and shifted the boundary between private and public, which has resulted in confusion related to the very meaning of privacy and made us question to what extent we should protect it anyway. Security issues continuously undermine the protection of privacy by imposing the need for more surveillance and control. Instead of being considered as a natural right, the right to privacy is constantly being contested.*

*In this paper it is analysed how new technologies altered our understanding of privacy and blurred the line between private and public spaces, imposing many challenges to protection of the right to privacy. I argue that these challenges are caused by the lack of definition of privacy and propose that we should rethink the concept itself in order to create a new operative definition which would enable better protection of this fundamental human right which is one of the most important pillars of modern democratic society and protects individuals from despotic controlling powers.*

Key words: *Privacy. The Right to Privacy. Technology. Human Rights. Security.*

---

\* Lecturer, Institute of Criminological and Sociological Research Belgrade, [ivana.stepanovic@gmail.com](mailto:ivana.stepanovic@gmail.com).

## 1. INTRODUCTION

The right to privacy is included in the *Universal Declaration of Human Rights*,<sup>1</sup> *International Covenant on Civil and Political Rights*,<sup>2</sup> and in the *European Convention on Human Rights*,<sup>3</sup> but there are numerous controversies around the meaning of the notion itself, as well as the demarcation line between the private and public sphere. One of the main reasons for this confusion is the rapid development of modern technology which has caused a major shift in our understanding of the notion of privacy. It almost seems that nobody knows the meaning of the word and this has big repercussions in the sphere of law.

The problem is not simply what does the word mean, but what does it mean to us. How much do we really care for privacy today? This issue is open to interpretation and sometimes debates arise even in courts when it gets difficult to make decisions just because parties disagree on the meaning and value of privacy. This fundamental human right constantly collides with the right to security and we are forced to choose sides and decide who is going to be the winner. While many think that the right to privacy should be defended as one of the pillars of democracy, others argue that privacy is overestimated since “we have nothing to hide”<sup>4</sup> thereby legitimising the ever increasing surveillance and control conducted by the military, police, secret services and even banks, medical institutions and business corporations. Colin Bennett pointed a way out of this conundrum when he stated that there is no consensus on how to define the notion of privacy, but there is some sort of “common agreement” that every human being needs it to a certain extent.<sup>5</sup> This is why the first task related to the protection of privacy should be accepting the arbitrariness connected to it and understanding it as a social construct, but also accepting it as something desirable.

It is commonly accepted that the development of digital tools of surveillance and control is the biggest privacy related problem of the postmodern society. Legal protection of privacy against technology is a problem apparently yet to be solved. In fact, technology dramatically

---

<sup>1</sup> The Universal Declaration of Human Rights, <http://www.un.org/en/documents/udhr/>, last visited 01 December 2014.

<sup>2</sup> International Covenant on Civil and Political Rights, <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, last visited 01 December 2014.

<sup>3</sup> European Convention on Human Rights, [http://www.echr.coe.int/documents/convention\\_eng.pdf](http://www.echr.coe.int/documents/convention_eng.pdf), last visited 01 December 2014.

<sup>4</sup> D. Solove, *Nothing to Hide, The False Tradeoff Between Privacy and Security*, Yale University Press, New Haven and London 2011, 47–210.

<sup>5</sup> C. J. Bennett, *Privacy Advocates: Resisting the spread of Surveillance*, The MIT Press, Cambridge, Massachusetts, 2008, 1.

transformed “the landscape on which laws are made”.<sup>6</sup> Since the 1970s, there has been a struggle to fit technology within a legal framework, but its constant development makes this task increasingly difficult.<sup>7</sup> Dealing with the consequences of technological improvement, which includes endless possibilities for “miniaturisation, convergence, interoperability and ubiquity”<sup>8</sup>, is an on-going project. For example, nowadays it is especially difficult to protect the right to private correspondence stated in the European Convention of Human Rights<sup>9</sup>. Prior to the invention of the telephone, the notion of correspondence referred to letters. Today it also refers to text messages and electronic mail. Electronic media are making privacy very hard to preserve. The main problem is that the antagonism between technology and privacy law is like a race between the tortoise and the hare: “No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay.”<sup>10</sup> This is why in order to find a solution to this problem, we must change the perspective and observe the problem from another point of view.

We must acknowledge that technology itself is not the problem, but the way we use it can be. As James Rule claims, blaming technology is definitely the wrong route to solving existing problems, as we are facing “uncomfortable and far-reaching choices among conflicting interests and basic social values”<sup>11</sup>. Firstly, to defend the right to privacy today means to require some sort of transparency of control. Establishing a fair and democratic control consists of, among other elements, a fairly transparent system within which citizens will not be secretly monitored and every individual would be able to see and control exactly where and to whom their data is shown. Control should be thoroughly regulated by law with special concern for human rights. Both concern for privacy and security must be respected without sacrificing one or another, but the right balance between the two can only be achieved within a particular context. Technology used for control must be used in a democratic and humane way. This means that there is nothing wrong with using technology in order to

---

<sup>6</sup> A. T. Keynon, and M. Richardson eds., *New Dimensions in Privacy Law*, Cambridge University Press, Cambridge 2006, 11.

<sup>7</sup> Council of Europe, *New Technologies: a challenge to privacy protection?*, Legal Affairs, Strasbourg 1989, 5.

<sup>8</sup> S. Gutwirth, et al., *Computers, Privacy and Data Protection: an Element of Choice*, Springer, Brussels 2011, v

<sup>9</sup> European Convention on Human Rights, [http://www.echr.coe.int/documents/convention\\_eng.pdf](http://www.echr.coe.int/documents/convention_eng.pdf), last visited 01 December 2014.

<sup>10</sup> D. Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Addison Wesley, Reading 1998, 9.

<sup>11</sup> J. B. Rule, *Privacy in Peril: How we are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, Oxford University Press, Oxford 2007, x.

maintain security, however, negative effects on individual freedom must be minimised.

Worryingly, technology is often used for morally wrong purposes that do not just violate privacy, but also have disempowering effects on individuals. We are often unaware of the ways in which we are being observed. It is exactly this unawareness that is making us frightened. Therefore the use of technology for the purpose of control should be regulated in such a way that it enables us to have greater control over life instead of jeopardising our actions.

## 2. BRAVE NEW PARANOID WORLD

Today's world is paranoid. We are constantly suspicious that we are being followed because we can never be certain of the ways in which we are being observed. Technology is in this sense invisible and unpredictable. There are several big fears linked to the rapid development of technology that humanity is now facing. One of them is the fear of a complete loss of privacy. There are some indications that this scenario may come true, and one of them is questionable privacy on the internet. As recognised magazines report: "Internet users have only recently begun to realise that every single thing they do online leaves a digital trace."<sup>12</sup> What seems to be the most disturbing fact is that people are being watched without even knowing it. Common sense suggests that it is deeply immoral.

What really seems worrying is the fact that surveillance is imperceptible, but not in the sense of Bentham's invisible watcher<sup>13</sup>. The "inspector" is replaced by spying devices such as mini flying cameras and radio frequency identification chips, of which we are not even aware of. In this sense, perhaps it is not just the government that poses a threat to our privacy. It seems that surveillance today is primarily linked to global capitalism, while in previous epochs it was performed mainly for the purpose of governmental control<sup>14</sup>.

In his book "The Transparent Society", David Brin lists surveillance gadgets that are not just used by the military, police and secret services, but are also available for civilians to use, such as infrared optics, camera robots and sound and video devices for indoor monitoring.<sup>15</sup> In

---

<sup>12</sup> The Economist, *Horror Worlds*, <http://www.economist.com/node/17388328>, last visited 01 December 2014.

<sup>13</sup> J. Bentham, *The Panopticon Writings: Edited and Introduced by Miran Bozovic*, Verso, London, 1995.

<sup>14</sup> S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly, Sebastopol 2000, 3.

<sup>15</sup> D. Brin, 7.

comparison to those devices, CCTV does not seem psychologically disturbing at all. Those small privacy intruders seem like an embodiment of Deleuze's theory about a society of control in which everyone controls everyone and instead of only one big brother, there are millions of them<sup>16</sup>. Invisible and uncontrollable, anarchistic surveillance is in this sense a real reason for paranoia. This invisible surveillance seems to be a by-product of capitalism. Everything, even surveillance, is available for sale. To avoid such potential dangers of capitalism, there should be laws that can effectively prevent the abuse of technology.

New technology also invites many other fears. One of them is that the machines will spin out of control and take over the world, just like in the film "The Matrix".<sup>17</sup> Other than that, there is a belief that people will begin to rely on machines to make decisions instead of them. Concerning privacy itself, there is a fear that surveillance systems will become so ubiquitous and unavoidable that individuals will not even have an opportunity to decide whether the data recorded on cameras can be used or not. Some theoreticians suggest that there is a big risk that "smart systems become black boxes, closed even to citizens who have the skills to understand them. Smart systems will make the world more transparent only if they themselves are transparent."<sup>18</sup> It is precisely the transparency of technology that must be provided in order to avoid the worst consequences of its development.

In order to get rid of our fears and restore the privacy that we have perhaps lost in the past decade, when all the major changes in the development of digital technology occurred, we must first acknowledge that technology itself is not the problem, for it can be used in both a right and wrong way. We can say that "technology produces adverse consequences for the individual, in particular his right to private life, his human identity, his dignity and his autonomy."<sup>19</sup> Furthermore, there are several characteristics of technology that are a potential threat to human rights. Firstly, networks are enabling the free transit of personal data. Secondly, integrated services digital networks (ISDN) are ensuring the collection of data through telemetric means without the intervention of the individual. Accordingly, "there is a danger of the surveillance of citizens, cutting an individual out of the information circuit, collecting personal information without the knowledge of the subject, exploitation of those data for different purposes, and finally, there is also fear of increasing the powers of

---

<sup>16</sup> G. Deleuze "Postscripts on the Societies of Control" *L'autre Journal* 1/1990, 3-7.

<sup>17</sup> The Economist, *Horror Worlds*, <http://www.economist.com/node/17388328>, last visited 01 December 2014.

<sup>18</sup> *Ibid.*

<sup>19</sup> K. E. Mahoney and P. Mahoney, *Human Rights in the Twenty first Century, A Global Challenge, Part 2*, Martinus Nijhoff Publishers, Dordrecht 1993, 803.

certain public and private bodies in the absence of democratic controls.”<sup>20</sup> Since there is not yet a proper way to protect human identity, dignity and privacy, we need some kind of principle-based approach to the application of information technology to protect those values.<sup>21</sup> Further development of technology can lead to even more severe intrusion into private life. Therefore, the problem must be solved legally and even on the constitutional level. Firstly, the problem must be recognised by governments. Secondly, new laws and rules must be introduced. In order to save the right to privacy, surveillance systems ought to be made transparent so individuals can be fully aware of the process.

### 3. THE FACEBOOK EFFECT

While on the one hand people are frightened of complete loss of privacy, on the other hand, they are clearly showing readiness to trade some of it. It can be argued that social networks have somewhat reshaped our attitude towards privacy. Many experts agree that internet users should act as if everything they do online – they do publicly.<sup>22</sup> Some of them have even suggested that a substantial shift in values has occurred and that our understanding of privacy significantly changed with the expansion of social networks. Even though people are aware of the fact that it is very hard to keep secrets in the virtual universe, they are actually revealing them every day as if they don’t really care about discretion as much as they used to. However, we must keep in mind that there is a big collision between our need to expose ourselves and protect our intimacy. In the words of Harry Blatterer, it seems that we are in “pursuit of visibility” while still wanting to have our privacy<sup>23</sup>.

Clashing desires for privacy and social recognition have often been misinterpreted. The founder of the most popular social network *Facebook* Mark Zuckerberg said that “people no longer have the expectation of privacy.”<sup>24</sup> Without a doubt, the enormous popularity of social networks shows that people have the need to expose themselves publicly and connect with each other. They enthusiastically share their intimacy on the

<sup>20</sup> *Ibid.*, 803–804.

<sup>21</sup> *Ibid.*, 804.

<sup>22</sup> S. Lohr, “How Privacy Vanishes Online”, *New York Times*, [http://www.nytimes.com/2010/03/17/technology/17privacy.html?\\_r=1](http://www.nytimes.com/2010/03/17/technology/17privacy.html?_r=1), last visited 01 December 2014.

<sup>23</sup> H. Blatterer, “Social Networking, Privacy, and the Pursuit of Visibility”, *Modern Privacy: Shifting Boundaries, New Forms*. H. Blatterer, P. Johnson and M. R. Markus, eds., Palgrave Macmillan, New York 2010, 73.

<sup>24</sup> B. Johnson, “Privacy no Longer a Social Norm”, *The Guardian*, <http://www.theguardian.com/technology/2010/jan/11/facebook-privacy>, last visited 01 December 2014.

*wall*: publishing photographs and thoughts, disclosing facts such as who they are in a relationship with, or who they are drinking coffee with. However, apart from the basic need to keep their privacy, there seems to be an equally powerful psychological urge to share their privacy with an audience. The reason people are willing to throw their private lives into the public realm is to get more friends or to become a more popular friend. The more information they share, the more attention they receive. This attention is so powerful and addictive that it significantly devaluates privacy.

However, it would be wrong to conclude that the fact that *Facebook* now has hundreds of millions of users means that privacy is an abandoned concept. Firstly, there are also very powerful campaigns against Facebook<sup>25</sup> and other social networks whose primary concern is privacy. Secondly, despite the fact that people are happy to disclose their private lives, they are still concerned with protecting their privacy. They want to have control over what they are sharing and with whom they are sharing. This is precisely what has been the most discussed topic related to social networks since they became widely popular.

The first time privacy became a problem for *Facebook* users, was when it introduced the “news feed” without previously announcing it. What used to be a private conversation among individuals suddenly became visible to all interconnected users. The problem here was not the fact that the new conception of communicating through this network included public conversations, but the fact that private correspondence had become open overnight without users’ permission: “When Facebook launched News Feed, it was changing the rules in the middle of the game, like a teacher who confiscates a passed note and forces the students to read it aloud.”<sup>26</sup> Paradoxically, the change that caused a scandal at the beginning later became the main characteristic of *Facebook*, which shortly became the most popular social network in the world. This proves that people are generally willing to put their private lives on display, but only under the condition that they are in control of this process.

According to this new understanding of privacy, influenced by the emergence of social networks, there is nothing wrong with revealing our private lives, as long as we are in control of this practice, and as long as it is regulated by the law. It is the users that should be able to decide where the border between private and public actually is. The fact that this boundary shifted after *Facebook* introduced the “news feed” confirms

---

<sup>25</sup> One of the world’s most famous *Facebook* saboteurs is a hacker group “Anonymous” that is, among other issues, concerned with privacy: <https://www.facebook.com/OffiziellAnonymousPage>, last visited 01 December 2014.

<sup>26</sup> D. E. Wittkower, ed., *Facebook and Philosophy*, Open Court, Chicago and La Salle 2010, 10.

that the distinction depends on the specific context. What seems to be confidential from one point of view can be considered as a public matter from another. This is yet another proof that privacy depends on a particular framework. In order to avoid violations of privacy, there must be strict rules regulating it: “What matters is not how many people know something, but whether the implicit rules of privacy in a social context are respected.”<sup>27</sup> Violation of privacy occurs when we do not give our consent to disclose certain information. As long as we are aware of the rules and accept them, privacy is not a problem.

Hence, the problem occurs when privacy is not clearly defined within a certain context, and when there are no policies or legislation to protect it. A few years ago, *Time* magazine published a cover story article about privacy on *Facebook* after the social network caused a scandal by exposing (selling) information on their users to the advertisers.<sup>28</sup> This was a clear sign that privacy on social networks needed to be meticulously defined and regulated by the law. This article was followed by several online protests of *Facebook* users. By doing this, protesters sent a clear message that they are aware of their entitlements to more privacy than they already have. They demanded to be in charge of not only how much information they share, but also with whom they share it. What was discovered is that the data users put on *Facebook* was being abused. Different companies were secretly controlling consumers. Extensive debates on privacy regarding social networks in the media were followed by significant changes in the so called “privacy policies” of *Facebook* and other companies. Once the border between private and public was shifted one more time, and a new set of rules regulating the social game were introduced, the dust settled again. This proves that the battle for privacy we have lost by joining social networks is not in vain.

It is precisely the invisible control, such as secret surveillance of *Facebook* users that poses the greatest threat to privacy nowadays. Under these circumstances, privacy is not even sacrificed for something more important, but is simply abused and should be protected by the law. In this context power is in the hands of company owners who are controlling their customers. It is crucial that this control be limited by laws and regulations that prevent abuse. Consequently, the proper balance between privacy and control, among other factors, depends on the rule of law and mechanisms for the protection of human rights.

---

<sup>27</sup> *Ibid.*, 8.

<sup>28</sup> D. Fletcher, “How Facebook is Redefining Privacy”, *The Time*, <http://www.time.com/time/business/article/0,8599,1990582,00.html>, last visited 01 December 2014.



#### 4. WORK IN PROGRESS

Establishing the desired proportionality between privacy and control is a process rather than a single achievement. Since privacy itself exists only within a particular context, determining the desired proportion between privacy and control should also be done contextually. This assignment should be dealt with within particular frameworks, since there cannot be only one operative principle that would resolve the relationship between privacy and control. The correlation between the two is too complex to reduce it to a simple dilemma of which one to choose, or which of them should be granted absolute primacy. Each context or milieu demands a different approach to the problem. However, debates about the right to privacy often start with the assumption that we should make a choice between the two priorities, namely – security and privacy. Nevertheless, making a definite choice seems to be impossible. Even though on the first thought security perhaps appears to be the more reasonable choice, there are cases that prove the opposite. Therefore we should not opt for one single solution, but rather for multiple options.

Some theorists such as David Solove argue that our society generally prefers pro-security arguments over those that favour privacy and suggests that exchanging the latter for the former is a “false tradeoff” that we should have not accepted, since both of them are essential values of a democratic society:

The consequences of the debate are enormous, for both privacy and security are essential interests, and the balance we strike between them affects the very foundations of our freedom and democracy. In contemporary times—especially after the terrorist attacks on September 11, 2001—the balance has shifted toward the security (...) But there’s a major problem with the debate: Privacy often loses out to security when it shouldn’t. Security interests are readily understood, for life and limb are at stake, while privacy rights remain more abstract and vague. Many people believe they must trade privacy in order to be more secure. And those on the security side of the debate are making powerful arguments to encourage people to accept this tradeoff.<sup>29</sup>

Therefore it is much more reasonable to decide on a balance between the two priorities than to entirely exclude one of them. This balance should be established by the rule of law and mechanisms for protection of human rights. However, even though legislation often seems satisfactory, there is little balance in practice. In reality, the court decision often amounts to devaluing privacy and sacrificing it to security. It does not seem too extreme even to say that the dilemma is often whether there

---

<sup>29</sup> D. Solove, 1-2.

should be privacy instead of searching for a rationale how to protect it, and to what extent it should be protected. There are many examples of a wrong proportion between privacy and security: “The law sometimes stringently protects against minor privacy invasions yet utterly fails to protect against major ones. For example, the Fourth Amendment will protect you when a police officer squeezes the outside of your duffel bag yet it won’t stop the government from obtaining all your Google search queries or your credit card records.”<sup>30</sup> This clearly shows why the right proportion should be looked for within a particular context.

Furthermore, there must be some general criteria that will decide what can be considered the proper balance between privacy and control within a particular context. What should certainly be taken into account is the well being of the whole society, but also the benefit of the individual. It is not only security, and consequently the right to life, that is in danger, but also the freedom and dignity of citizens. While taking care of public security, disempowering consequences for the individual should be avoided. In other words, perhaps the optimal strategy in the majority of cases would be to maximise security and minimise privacy violations. However, both benefits and losses should be carefully calculated.

Even though the two values often collide when collective and individual interests meet, it would be wrong to conclude that privacy is merely an individual or even a selfish concern. As David Solove further argues: “Balance shouldn’t just focus on your privacy – it should weigh privacy of location for everybody in society. Privacy should be understood as a societal value, not just an individual one.”<sup>31</sup> In fact, a good society can perhaps be characterised as one in which individual requirements and the needs of the whole community are not divergent. Accordingly, just as control should not be seen simply as an unnecessary restraint of an individual (because it is for his/her own benefit), neither should privacy be perceived as needless limitation of the social order.

It is through the mechanisms for protection of human rights that the balance between privacy and control is being created and sustained. For example, mechanisms for the protection of personal data limit controlling powers, while at the same time regulation of data flow across borders for security reasons limits privacy. But even though regulations are constantly being improved, there are many problems yet to be solved, such as privacy on internet. The rapid development of technology generates many problems related to both privacy and security. Constant change is hard to grasp by the legislature, which is why remedies are often created *post hoc*.

---

<sup>30</sup> *Ibid.*, 2 3.

<sup>31</sup> *Ibid.*, 47.

In the process of creating legal and human rights remedies, finding a proper balance between privacy and control, rather than making a definite choice of preference between them should be the first guiding principle. Furthermore, this should be done in accordance with democratic principles. Controlling powers must be constantly pacified and limited so that they are democratic rather than despotic. In other words, there is nothing substantially wrong with control if it is kept transparent and actively and lawfully restrained. Control should only be conducted with respect for privacy to a certain limit which must be determined contextually. The vital criteria of this double limitation is the benefit of both society as a whole and on the individual level, rather than in particular power formations. What should be prevented is that control/power becomes centralised and repressive. In this sense, there is a constant danger that the institutions of capitalism could become centres of repressive power that conduct surveillance without any respect for privacy. This is why the rule of law and human rights must constantly create and maintain the democratic balance. It is a work in progress.

## 5. CONCLUSION

It seems that the problem with the right to privacy is obvious: development of technology has led to uncontrollable and invisible digital surveillance. Legal protection is always a few steps behind the mechanisms of control and unable to deal with the growing number of problems related to protection of privacy.

However, the underlying problem is our understanding of privacy. There is no consensus on what we mean by it. Moreover, there are also contrasting views on how it should be protected and even whether it should be protected at all, or perhaps sacrificed for security. Therefore privacy needs to be both redefined and reassessed. It is crucial that we first acknowledge it as a social construct. Instead of struggling to define it, we should accept the fact that it is impossible because its meaning depends on a particular context. Furthermore, we should let go of the classical libertarian definition according to which it is a negative right and the private sphere should be free from any governmental interference<sup>32</sup>. However, it is equally wrong to marginalise privacy and surrender to the faceless power of the post-modern Deleuzian “*societies of control*”<sup>33</sup>.

The solution lies somewhere in the middle, between radical individualism and capitulation to total control. This means that privacy and

---

<sup>32</sup> J. Locke, *Two Treatises of Government, The works of John Locke*. In Ten Volumes. Vol. V. London 1823.

<sup>33</sup> G. Deleuze, “Postscript on the Societies of Control”, *L'autre Journal*, 1/1990, 5.

control should no longer be seen as contradictory, but rather as complementary values. They should limit each other and therefore prevent negative consequences of excessive freedom or potentially oppressive controlling power. Balance should be sought contextually, since it is impossible to find proportionality that would fit universally.

However, it is not just any kind of control that is compatible with privacy. Contemporary societies aspire to democratic control which should be understood in relation to the notion of power. Democratic control aims to pacify existing power relations in order to prevent any despotic powers. In this sense democratic control is preventive, and amounts to surveillance that is mere monitoring without aspirations to be manipulative in any way. But even this democratic control needs to be limited by the respect for privacy, since without this restriction it can easily become autocratic. On the other hand, privacy limited by control which preserves peace and security enables more control over life. In deciding upon the desirable balance between them, regulated by the rule of law and human rights mechanisms, we should opt for the solutions which are beneficial for both society and the individual.

When it comes to modern technology, the process of monitoring data should be visible to citizens and there should be some kind of “principle of reciprocal benefits” which means that both controlling powers and common citizens not only have access to data but also both gain something from the process of control.

Regarding the conflict between privacy and security, the optimal solution is to ensure security while at the same time minimising violations of privacy. Disempowering consequences of surveillance on individuals should be avoided, for providing public good is not the only condition for maintaining a just society. This is particularly important with regards to data surveillance, which now poses the biggest threat to privacy. It seems that a Kafkaesque bureaucracy nightmare is now more real than ever, considering that identity thefts as well as buying and selling data have become an everyday practise. Even espionage is no longer a job done only by the secret services and military. This is why limiting control by privacy rights is vital for every democratic society. In this sense technology should play for both sides: protecting privacy on the one hand and preserving security on the other.