Diametros 18 (2021), 70: 64–77
doi: 10.33392/diam.1544

How Is Political Privacy Different From Personal Privacy? An Argument From Democratic Governance

– Aleksandra Samonek –

Abstract: In this paper I discuss the political value of the right to privacy. The classical accounts of privacy do not differentiate between privacy as the right of a citizen against other citizens vs. the right to privacy as the right against the state or the government. I shall argue that this distinction should be made, since the new context of the privacy debate has surpassed the historical frames in which the intelligence methods used by governments were comparable to those available to individuals. I also present cases in which political privacy serves as an instrument of protecting important collective agendas exceeding the context of personal privacy. I argue that due to its function, political privacy should be considered a necessary element of democratic governance with the rule of law, imposing legal bounds on governments' discretionary actions.

Keywords: privacy, the right to privacy, democracy, rule of law, democratic governance, political privacy

Published online: 15 December 2021

1. Introduction

Privacy concerns have driven legal scholarship debates at least since the beginning of the Golden Age of photojournalism. Following the publishing standards and market success of *Berliner Illustrirte Zeitung* in 1901, journals started printing photographs inside each issue, thus introducing the modern news magazine format. Warren and Brandeis[1] soon put forth an argument against photographic press coverage, claiming that the damage to

Aleksandra Samonek
Jagiellonian University
Institute of Political Science and International Relations
ul. Reymonta 4
30-059 Kraków, Poland
Institute of Philosophy
ul. Grodzka 52
31-044 Kraków, Poland
Université Catholique de Louvain
Institut Supérieur de Philosophie
Place Cardinal Mercier 14, bte L3.06.01
1348 Louvain-la-Neuve, Belgium
aleksandra.samonek@uclouvain.be,
asamonek@protonmail.com

[1] Warren, Brandeis (1980).

personal privacy it incurs leads to "spiritual harm," which makes a person incapable of meaningfully partaking in social life and maintaining control over their everyday affairs.

Ever since, each new type of technology introduced the public to unfamiliar anxieties and inconveniences. Social networks, one of the most recent technological developments which fell under public scrutiny, offer research possibilities that contribute to a better understanding of various social issues, for example, through tracking the racial and social factors in unemployment,[2] or investigating the dynamics of participatory opinion-making.[3] At the same time, social networks have been shown to negatively impact self-esteem[4] and have become a powerful vehicle for spreading fake news[5] that undermine reliability of the social channels for sharing information. The evaluation of technological developments is often portrayed as a trade-off between the effectiveness of performance and privacy.[6] Is this trade-off essential to the modern conflict between technology and privacy?

In this paper I draw attention to what is in my opinion the most central aspect of the right to privacy in modern times, that is, the political value of the right to privacy. I propose that we distinguish between two types of privacy, namely, personal privacy understood as the right of a citizen against their fellow citizens, and political privacy understood as the right against the state or government institutions. What we gain with the dualist approach to privacy are much more specialized and effective legal and political tools that protect our privacy in each domain – personal and political, that is, against our pars or against our governments. For the sake of simplicity, I will not discuss here the position of surveillance capital in this setup. Surveillance capitalists, such as Facebook or Google, deal with user data treated as raw material, while sometimes boosting the influence of the governments on the surveillance landscape, either nationally or internationally. Thus, the position of the surveillance capital adds yet another layer of complication, which, if elaborated on, would detract from the main point of this paper. For those interested in how surveillance capital threatens our privacy, a detailed exposition such as that by Zuboff[7] will be much more informative than a summary that could be given in this paper.

2. Conceptualizing privacy

Anita Allen,[8] Ruth Gavison,[9] and James H. Moor[10] subscribed, albeit in various ways, to the idea that privacy is a matter of restricting access to persons and information about persons. This view avoids various fatal counterexamples to which previous theories of privacy were susceptible (for a detailed argument concerning some of the more prominent historical accounts of privacy, see Moor's paper).

[2] Reingold (1999).
[3] Porter, Hellsten (2014).
[4] Vogel, Rose, Roberts et al. (2014).
[5] Lazer, Baum, Benkler et al. (2018).
[6] Cf. Rindfleisch (1997); Zhang, Shu, Cheng et al. (2016).
[7] Zuboff (2019).
[8] Allen (1988).
[9] Gavison (1980).
[10] Moor (1990).

According to James H. Moor, an individual or a group have privacy in a situation if and only if in that situation the individual or a group, or information related to them, is protected from intrusion, observation, and surveillance.[11] Therefore, a *private situation* is a situation in which we are protected from intrusion, observation, and surveillance. The question of maintaining privacy can be reformulated in terms of this definition. It will be of the form: which situations are private to us, and which are not? The division into naturally (descriptively) private situations and normatively private situations proposed by Moor[12] can be adapted for the political context of privacy and allows avoiding certain irrelevant counterexamples which are otherwise bound to come up in the debate over the right to privacy in any context.

A naturally private situation is one in which a person is, as a matter of fact, free from intrusion, observation, or surveillance. These situations were also labeled as "descriptive privacy."[13] Examples of such situations are walking alone in the forest or enjoying a quiet evening at home with friends when we are not being observed or interrupted by intruders.

This type of privacy is quite independent from normative privacy. Sometimes the loss of natural privacy constitutes an invasion of privacy and sometimes it does not. Normatively private situations are those in which we either do or do not have natural privacy, but privacy is due to us because of a moral, legal, or pragmatic reason. Thus, a truly interesting question for the debate over the right to privacy is the following: which situations are normatively private? That is, in which situations the protection against intrusion, observation and surveillance is due? James H. Moor saw this question as particularly difficult to answer because, on the one hand, the catalog of normatively private situations seems to be determined culturally, and so one must consider intercultural variance and changes in the popular opinion which happen over time, but on the other hand, "the nature and kind of situations which ought to be private is open to rational and moral argument."[14]

My proposal is to rely on the distinction between personal and political aspects of the right to privacy to answer the question about which situations are normatively private in a political context. While there may exist separate instances of regulations concerning exclusively personal or political privacy violations, legal doctrine, as well as legal and political philosophy still lack proper exposition of the right to privacy as *dual* in nature. I argue that while personal privacy is indeed regulated culturally, political privacy is not, as long as the culture involves the social legitimization of power.

In modern philosophy, politics, and policymaking, a postulate that the rule of law should be respected or that the government of a nation should be legitimate is not a morally contested claim. While we demand privacy based on moral or legal justification in situations related to the personal sphere, in those related to the political domain our demands will be based on political necessity. The normatively private situations should therefore be those in which our free or anonymous choice (or action) is needed to guarantee our unrestricted participation in the social legitimization of power.

[11] Ibidem: 76.
[12] Moor (1997).
[13] Tavani, Moor (2001): 6.
[14] Moor (1990): 77.

3. Privacy infringement vs. surveillance

Numerous theories describe privacy as an *erga omnes* right, that is a right enforceable against anyone and everyone infringing on it. Examples of such theories include the non-intrusion theory of privacy,[15] the theory of privacy as freedom to act,[16] the theory of privacy as control of information,[17] the theory of privacy as undocumented personal knowledge,[18] and the aforementioned restricted access theory of privacy.[19] In all those classical accounts of privacy, no distinction is made between privacy as a right against fellow citizens and privacy as a right against the government institutions.

Although institutions protecting the right to privacy were historically understood as a means of preventing infringement by virtually anyone, the emergence of mass surveillance technologies spurred the *de facto* diversification of the scope of privacy protection. In the past, the methods and capabilities for interfering with the affairs of the individual were similar in the case of the agents of the government and in the case of fellow citizens who decided to spy on their neighbors or colleagues. The difference was mostly found in the magnitude of surveillance efforts, as the resources of the government greatly exceed those of an individual. Adequately, spying done by fellow citizens has gained the name of *privacy infringement*, while spying by the government agencies and the surveillance capitalists is known as *surveillance*. However, despite there being two very distinct powers working against privacy, the notion of privacy itself remains uniform, and with immediate negative consequences.

In the legal systems of many EU countries, we are provided with laws and law enforcement agencies aimed at protecting our right to privacy as infringed by our fellow citizens or private business agents, while at the same time we have very limited means of protecting our right to privacy as infringed by the authorities, understood as either a government branch or another surveillance institution authorized or subsidized by the state. Although general protection clauses exist, such as Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and although privacy protections were integrated into the Treaty on European Union (TEU) by the Treaty of Lisbon, the implementations of the protections at the national level are largely insufficient, leaving very little actionable responses available to the citizens and allowing for rather limited judicial control over state surveillance. This trend is representative of many developed countries, which rely on national data protection authorities or information commissioners in safeguarding citizens' privacy when the state is usually not involved in surveillance.

In the following section, I will elaborate on how surveillance – both targeted and mass surveillance – plays a role in inhibiting the political activity of groups and communities, which in turn blocks the development of collective social agendas, such as climate protection.

[15] Warren, Brandeis (1980).
[16] Moor (1990): 74.
[17] Schoeman (1984): 209; Westin (1968, 2003); Beardsley (1971).
[18] Parent (1983).
[19] Allen (1988); Gavison (1980); Moor (1990).

4. Political privacy as a protection of collective agenda

Although political privacy serves a multitude of functions from the democratic standpoint, its one important aspect is the protection of the rights of minorities. In this sense, political privacy may be viewed as a collective right of groups or communities of citizens. More generally, political privacy protects collective social agendas and rights, and the context of national security plays a role here as well.

Wolfers[20] observed that both terms, *national security* and *national (or public) interest* are ambiguous, and likely to mean different things to different people. Certain events, such as the 9/11 attacks bring about systematic transformations in national security. For instance, Zelikow[21] gave an account of the national security transformation planned by the Bush administration after the World Trade Center attacks. His description of the direction of the transformation included clear colonial and hegemonial ambitions, referred to as the "unique responsibilities [of the USA] as the greatest power in this pluralistic world."[22] Hence, the implementation of the national security as performed by the state administration may be, and, in fact, often is, ideology-driven, at least to a certain extent.

New elements may be included in the scope of national security agendas as particular problems start being perceived as a threat to the public or national interest. For instance, Levy[23] argued that global environmental degradation was a threat to the USA while defining three forms of connection between the environment and security, existential, physical, and political.[24] However, as I am about to argue, non-violent activism, climate or otherwise, as well as general political involvement of the citizens *cannot* be included among the security threats in a democratic state when no further indication of threat is involved. In other words, a state which aspires to be called democratic must formulate its security agenda in a way which makes normal political activity, including protests and civil disobedience, both possible and feasible.

Given these assumptions, in the case of, e.g., recent controversies surrounding climate activism in France,[25] the measures taken against the activists and citizens do not fit into the notion of protecting national security, at least not in conjunction with the democratic state. That is, state surveillance, including mass surveillance, often has little to do with the national or public interest understood within the frame of democracy. What is more important here, however, is that the case which I am about to present below does not in fact concern a clash between strictly personal privacy and national or

[20] Wolfers (1952): 481.
[21] Zelikow (2003).
[22] Ibidem: 19.
[23] Levy (1995): 36.
[24] The existential link relies on the relationship between certain aspects of the global environment and the US national values, which are so strong that they give rise to security interests. The proponents of this view are, among others, Jessica Tuchman Mathews and Norman Myer (cf. Levy (1995: 36)). The physical link means that the global environmental degradation has consequences which may arise as physical threats to US security. Finally, the political link is indirect and includes issues such as the appearance of environmental refugees, resource wars, etc. Surprisingly, Levy considered the political link between the environmental degradation and national interest as "the weakest substantive threat to US security".
[25] Sauer (2019).

public interest. Rather, the privacy of individuals is treated as a collection of pressure points, which allow the state to diminish and neutralize a *collective* agenda of a group of citizens. Political privacy of the collective can be eliminated by targeting the individuals who engage in it. With mass surveillance, simple network analysis allows the state to identify those individuals whose neutralization will be most cost-effective. For instance, as will become clear in the case to follow, the French state decided to force disengagement from the members of the legal team of COP21 through home arrests, as well as physical and communications surveillance.

For this reason, I argue that political privacy must be considered as driving a collective right, as well as individual rights. In recent years, there has been a surge in collective rights programs, including in the debates on cultural appropriation and slavery reparations. Although there are stark differences between the problem of privacy and those of cultural appropriation or slavery and its consequences, note that the emergence of the idea of a collective right is relatively recent, and so is the associated theoretical apparatus. As a result, the way in which the collective rights programs are formulated will be similar, often relying on similar theoretical infrastructure, even if the nature of the rights varies from case to case.

The following case concerns a climate activism movement in France, focusing on an organization called COP21. Non-Violent Action COP21 (ANVCOP21) is a grass-root movement of French citizens who fight climate change and the social injustices it engenders. Their methods include many forms of non-violent resistance and protest, including resisting projects and policies which have a negative impact on the climate. In some cases, the group relies on civil disobedience; for instance, removing portraits of Emmanuel Macron from the walls of town halls across France to draw attention to what the group sees as the president's failure in terms of climate leadership. The movement began in February 2019 and involved 276 activists by April that year.

The response of the French authorities to the movement's actions was immediate. By April 2019, 20 people were prosecuted, 22 detained and 16 police searches carried out to stop the takedown of presidential portraits. What is even more surprising, however, is that the group's non-violent protest was almost immediately classified as an act of domestic terrorism by the French police. Consequently, the *Bureau de la Lutte Anti-terroriste* (BLAT), the central office of counter-terrorism activity in France, started investigating the ANVCOP21 members and group operations.

Sauer[26] indicated that the hard response of the French government has a wider context in both France and the EU. In February 2019, the High Commissioner for Human Rights, Michelle Bachelet, recommended the UN to investigate France for the excessive use of force against the *gilets jaunes* ("yellow vests") protesters. In December of the same year, the commissioner put forward a statement of support for climate activists. However, the French government has been expanding its discretion in using anti-terrorism measures and surveillance for a while, despite the calls for limitations put forward by political experts and legal scholars alike. Back in 2016, journalists and analysts called for the prevention of arbitrary policing by adopting prior judicial controls over anti-ter-

[26] Ibidem.

rorism measures. The state of emergency in France (in force from November 13, 2015, to November 1, 2017) only allowed for an *a posteriori* judicial review and provided the time needed to pass the new, harsher counter-terrorism legislation. Together with the November 2015 law on surveillance of international electronic communications, which increased the state's capability for collecting, analyzing, and retaining communications content and metadata without authorization or judicial review, the new counter-terrorism measures created an impassable bottleneck for the political activity of citizens.

It is an open question of how, if at all, the political activity of citizens, especially in the form of protest or non-violent disobedience, is feasible under the current application of French counter-terrorism laws and policing measures. In light of the disproportional use of force and suppression of even the most benign forms of protest, how can the political activity typical of the democratic state with the rule of law continue in France? The UN called for France not to extend the state of emergency beyond February 26, 2016, but the call was unsuccessful. The UN experts, including David Kaye, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and Maina Kiai, Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association, and others, spoke against the house arrests of the French climate activists which were made possible by the state of emergency in 2015 and 2016. They also warned the French government against abusing the capabilities stemming from the state of emergency:

> While exceptional measures may be required under exceptional circumstances, this does not relieve the authorities from demonstrating that these are applied solely for the purposes for which they were prescribed, and are directly related to the specific objective that inspired them.[27]

In January 2021, a new wave of mass protests erupted in France over a strengthening of security laws, including a bill that makes it a criminal offense to film and publicize images of police during operation, thus also making it impossible to share and publicly scrutinize images proving acts of police brutality. From a purely technical perspective, the methods of surveillance currently in operation and being used against the citizens in France are well documented in cases of climate activists. In a crowd-funded groundbreaking documentary on privacy and surveillance entitled "Nothing to Hide," two Berlin-based journalists, Mihaela Gladovic and Marc Meillassoux[28] included testimonies of French and German activists, showing that both targeted and mass surveillance have become a standard in the state's approach to activism.

Joël Domenjoud was one of the 26 COP21 activists put under house arrest during the state of emergency in France. Notably, Domenjoud was part of the legal team of COP21 and supported the activists' work within the organization's non-violent agenda. The level of surveillance employed against Domenjoud made his participation in the legal team impossible. Since all communications from and to Domenjoud were monitored, it was impossible for the team to coordinate and act without police supervision.

[27] OHCHR (2016).
[28] Meillassoux (2017).

The near complete surveillance of communications, including all electronic and mobile communications, of this particular activist, not only neutralized his impact within the organization and against the state, but also prevented him from safely using email and other electronic channels to contact his friends and family, and limited his use of electronic devices in general. This in itself constituted a form of repression, since the fact of being under observation was clear to him from a certain point in time, and no countermeasures were available to him. Physical surveillance was employed as well, with the police following Domenjoud wherever he went. Whether this measure was meant as actual surveillance or simply an intimidation strategy is an open question. However, Domenjoud's surveillance was most likely initiated based on his association with COP21 and as such, did not stem from *mass* government operations. Moreover, note that the COP21 was explicitly non-violent, so it should be considered benign from the perspective of national security. Hence, any use of security measures in cases of COP21 protests was purely instrumental on the side of the French state. In this sense, the case of COP21 does not illustrate any aspect of the conflict between political privacy and the actual national or public security.

The situation was different in the case of Andrej Holm, a German sociologist working on the topic of gentrification in Berlin, who was surveilled by the German intelligence police agency (*Bundeskriminalamt*, or BKA) based on the keywords in his internet searches, which included "gentrification," "reproduction," and "Marxist-Leninist." Based on seven keywords, all common words for a researcher of his specialization, Holm was placed under full-fledged online surveillance in 2006 and suspected of being a terrorist in a militant group. Together with Holm, a network of other people, including his friends and colleagues, was likewise surveilled. This group included activist and political scientist Anne Roth. And since this particular surveillance case was both documented (thanks to the German right to notification), and untargeted – based on a purely algorithmic evaluation of mass records of online searches – it is in some sense much more serious, politically speaking, than the case of Joël Domenjoud and the rest of COP 21 activists.

However, an important aspect of the French surveillance landscape is that no right of notification is available. Given the flow of technologies within the EU, it is safe to assume that very similar *mass measures* are used against activists, scholars and other citizens in France as well. Therefore, any citizen undertaking an activity or research in areas or topics which may be *problematic* to the French state, should, as a matter of fact, expect to be placed under surveillance similar or exceeding that used against Holm, Roth, and others in Germany.

5. Shifting priorities vs. control over information

Another element of the political dimension of privacy is the protection against discretionary policy setting by the government. Here again the case of France shows that surveillance technologies are often used as a means of control and suppression. One of the fundamental reasons why robust surveillance practices are viable in France is the lack of protection against surveillance in the French civil and constitutional law. Another

important observation concerning the *de facto* evolution of state surveillance in France was offered by Gillis.[29] From the historical perspective, state surveillance, despite being marketed to the public as a class of measures targeting primarily violent crime, including major crime such as terrorism, has been demonstrably effective in preventing property crime in the second half of 19th and 20th century, but its impact on violent crime in urban environment has been minimal. Moreover, based on extensive historical and statistical evidence, Gillis[30] indicated that:

> A reversal of the equations shows that crime rates had little or no effect on the growth of national policing. This, and historical evidence, suggests that state surveillance expanded less from a specific intent to control crime than from a broader interest in repressing "dangerous classes," new repertoire of social protest, and political challenge to the state.

Tréguer[31] pointed out that the French legislative proposals, especially since the French 2014 Anti-terrorism Law, "greatly reinforced the power of intelligence and police agencies by circumventing traditional criminal procedures." A clear shift can be observed in the development of surveillance state in France in the recent years: from a court-controlled, publicly mandated surveillance, the country is moving towards a covert, discretional toolbox of policing solutions. As for the 2015 Intelligence Act, Mastor[32] observed that the focus of the French surveillance regulations was not on counterterrorism, a solution which would require judicial oversight of policing and surveillance activity, but aligns with the prioritization of property protection in French state surveillance efforts identified by Gillis.

France is certainly not an exception in terms of how governments exercise control over their people, while their policy priorities are shifting towards capital protection. Surveillance technologies used by national governments are often aided by surveillance capital, enabling a wide range of methods of obtaining and exploiting private information, including recording phone calls, scanning mobile networks using voice recognition, reading private emails and text messages, secretly censoring web pages, tracking a citizen's detailed movement using GPS, and changing email contents while *en route* to a recipient. Multiple reports on mass surveillance technologies put together by the Electronic Frontier Foundation describe how authoritarian and democratic governments alike rely on surveillance methods to facilitate human rights abuses in countries like China, Syria, or Egypt.[33] Those methods only represent a small proportion of the potential to make use of the leverage associated with personal information about a person, be it directly incriminating or not.

On the level of strategy and decision-making, accessing someone's personal information ultimately yields control over their motivation system. Depending on the

[29] Gillis (1989).
[30] Ibidem: 307.
[31] Tréguer (2016): 34.
[32] Mastor (2017).
[33] Hassine (2016).

type and content of the information, we may gain leverage in a negotiation or provide strong incentives for making a specific decision. The surveillance technologies from before the mobile and web communication era were not quite as comprehensive as their modern successor. Spying on a person previously required resources, like manpower, funds, and planning. Consequently, only certain chosen individuals could be spied on, be it by the government or by their fellow citizens. With mobile and web technologies at hand, spying on an individual does not require manpower, incurs negligible costs, and does not require planning.

Permanent records of electronic communication allow agents to access the existing database and search it for personal information of a person of interest. By the same token, the controlling agent can often gain instant access to personal communications and their whereabouts *via* the back door which many companies provide to the surveillance authorities either secretly, like in the case of Apple, Yahoo, and others in the USA, or completely openly as do all the companies operating in China, in particular Weibo and WeChat. Therefore, in the present state of technology, control over an individual's decision-making can be obtained at almost no cost.

6. Conclusions

Moor suggested that limited intrusion into our privacy may have positive effects for fields like epidemiology or law enforcement.[34] After all, the more information we provide to the state, the more effective that law enforcement efforts become. However, Moor also enlists certain indispensable goods which can only be obtained by protecting privacy, like enhancing personal liberty, maintaining control over one's own personal development, and avoiding emotional and psychological harm.

Unlike Moor, who stressed the intrinsic value of personal privacy and its protection,[35] I take an instrumental approach to political privacy, assuming its central role in creating the basis for social organization and securing the rule of law. My considerations fall into the tradition of approaches worked out by philosophers like Stanley Benn,[36] Charles Fried,[37] James Rachels[38] and Deborah Johnson.[39] All of them saw the *instrumental value of privacy* in facilitating basic social and personal interactions and development. Benn and Gaus saw privacy as a display of respect given to someone as a person. Stripping someone of their privacy is therefore meant as an act of dehumanization. Deborah Johnson said that privacy increases personal autonomy,[40] while Rachels claimed that privacy is necessary for creating diverse social relationships.[41] Even Moor, who defends the intrinsic value of privacy, sees its violation as a type of "spiritual harm."[42] My ap-

[34] Moor (1990): 77–78.
[35] Ibidem: 81.
[36] Benn, Gaus (1983).
[37] Schoeman (1984).
[38] Rachels (1975).
[39] Johnson (1985).
[40] Ibidem: 67.
[41] Rachels (1975): 292.
[42] Moor (1990): 71.

proach embraces the instrumentalist view of privacy, while making explicit its political significance.

However, I propose to consider privacy not as an instrument of *personal* liberty or facilitating social interaction, but rather as a means of maintaining the ability of a society to influence its government and authorize its decisions. Taking away citizens' privacy is an attack on the pillars of social legitimization of power, an essential component of the rule of law. If we understand the rule of law as a facilitator of political circumstance in which the behavior of individuals and institutions is bounded by the law, avoiding discretionary decisions becomes central to protecting the social values and collective agendas. In the case of political privacy, the best way to protect these agendas is *via* privacy protection, especially through blocking mass surveillance, but also control over targeted surveillance, such as that of COP21.

Although the rule of law is a widely contested concept as to its precise explication, because of its frequent occurrence in the public justifications of the legitimacy of the government it has become a standard condition for legitimization of governments worldwide, even in the countries which are themselves far from a democracy.[43] In its full generality, the rule of law can be interpreted as a principle of constraining the behavior of government officials and citizens so that the nation is governed by the law and not by decisions of individuals who occupy the public office at a given moment. The rule of law is equally important to liberal and anti-liberal philosophers, to supporters and opponents of a democratic state.[44]

However, no government can boast social legitimization of its power in the context where its officials are *always* capable of finding incriminating evidence against any citizen, turning the justice system into a sort of on demand service for the state. And yet this is the case in all countries whose mass surveillance apparatus and methods are sufficiently advanced. Therefore, several legal institutions have been significantly weakened since the emergence of mass surveillance technologies,[45] including, but not limited to, the right against self-incrimination.

In this paper I argued for an account of privacy as a political right which facilitates a clearer discussion on the scope of the permissible surveillance of citizens conducted by the government. Taylor pointed out that limitations must be put on governments' ability to conduct mass surveillance.[46] My approach offers merely the first step towards creating these limitations *via* setting a clear theoretical distinction between political and personal aspects of privacy. I propose that we consider as normatively private those situations where our free or anonymous choice (or action) is needed to guarantee our unrestricted participation in the social legitimization of power. Accepting such a formulation of political privacy only requires that we accept the rule of law as a necessary condition for the operation of modern state. The concept of political privacy avoids several other commitments, such as prioritizing personal comfort or freedoms, or ascribing inherent

[43] Tamanaha (2004): 3.
[44] See for example: O'Donnell (2004); Przeworski, Maravall (2003); Raz (1977); Scalia (1989); Engelstein (1993).
[45] Carrera et al. (2015).
[46] Taylor (2017): 326.

value to them. My approach is compatible with the instrumental view of privacy, at least in its political dimension, leaving the door open for justifying privacy in its interpersonal, culturally dependent aspect.

Acknowledgements. The author would like to thank the anonymous Referees and Prof. Dorota Pietrzyk-Reeves for their helpful comments and questions, as well as the editorial team of "Diametros" for their suggestions for significant improvements in the paper.

References

Allen A.L. (1988), *Uneasy Access: Privacy for Women in a Free Society*, Rowman & Littlefield Publishers, Totowa.

Beardsley E. (1971), "Privacy: Autonomy and Selective Disclosure," *NOMOS. Yearbook of the American Society for Political and Legal Philosophy* XIII: *Privacy*: 56–70.

Benn S.I., Gaus G.F. (eds.) (1983), *Public and Private in Social Life*, St. Martin's Press, New York.

Carrera S., Fuster G.G., Guild E. et al. (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, CEPS, Bruxelles.

Creemers R. (2018), "China's Social Credit System: An Evolving Practice of Control," URL = https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 [Accessed 18.11.2021].

Engelstein L. (1993), "Combined Underdevelopment: Discipline and the Law in Imperial and Soviet Russia," *The American Historical Review* 98 (2): 338–353.

Gavison R. (1980), "Privacy and the Limits of Law," *The Yale Law Journal* 89 (3): 421–471.

Gillis A.R. (1989), "Crime and State Surveillance in Nineteenth-Century France," *American Journal of Sociology* 95 (2): 307–341.

Hassine W.B. (2016), "The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online," Electronic Frontier Foundation Report, URL = https://www.eff.org/files/2016/04/28/crime-of-speech.pdf [Accessed 12.12.2017].

Johnson D.G. (1985), *Computer Ethics*, [in:] L. Floridi, *The Blackwell Guide to the Philosophy of Computing and Information*, Blackwell Publishing, Malden.

Lazer D.M., Baum M.A., Benkler Y. et al. (2018), "The Science of Fake News," *Science* 359 (6380): 1094–1096.

Levy M.A. (1995), "Is the Environment a National Security Issue?," *International Security* 20 (2): 35–62.

Meillassoux M. (2017), "Nothing to Hide," a documentary film, URL = https://nothing-tohidedoc.wordpress.com/ [Accessed 1.11.2017].

Moor J.H. (1990), "The Ethics of Privacy Protection," *Library Trends* 39 (1 and 2): 69–82.

Moor J.H. (1997), "Towards a Theory of Privacy in the Information Age," *ACM SIGCAS Computers and Society* 27 (3): 27–32.

Newman J. (2009), "Google's Schmidt Roasted for Privacy Comments," URL = https://www.pcworld.com/article/184446/googles_schmidt_roasted_for_privacy_comments.html [Accessed 15.11.2017].

O'Donnell G.A. (2004), "Why the Rule of Law Matters," *Journal of Democracy* 15 (4): 32–46.

OHCHR (2016), "UN Rights Experts Urge France to Protect Fundamental Freedoms while Countering Terrorism," OHCHR Press Release, URL = https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?LangID=E&NewsID=16966 [Accessed 18.11.2021].

Parent W.A. (1983), "Privacy, Morality, and the Law," *Philosophy & Public Affairs* 12 (4): 269–288.

Porter A.J., Hellsten I. (2014), "Investigating Participatory Dynamics through Social Media Using a Multideterminant "Frame" Approach: The Case of Climategate on YouTube," *Journal of Computer-Mediated Communication* 19 (4): 1024–1041.

Przeworski A., Maravall J.M. (eds.) (2003), *Democracy and the Rule of Law*, vol. 5, Cambridge University Press, Cambridge.

Rachels J. (1975), "Why Privacy is Important," *Philosophy & Public Affairs* 4 (4): 323–333.

Reingold D.A. (1999), "Social Networks and the Employment Problem of the Urban Poor," *Urban Studies* 36 (11): 1907–1932.

Raz J. (1977), "The Rule of Law and its Virtue," *Law Quarterly Review* 93 (2): 195–211.

Rindfleisch T. (1997), "Privacy, Information Technology, and Health Care," *Communications of the ACM* 40 (8): 92–101.

Sauer N. (2019), "French Counter-Terrorism Targets Climate Activists," URL = https://theecologist.org/2019/apr/04/french-counter-terrorism-targets-climate-activists [Accessed 12.12.2019].

Silverglate H. (2011), *Three Felonies a Day: How the Feds Target the Innocent*, Encounter Books, New York, London.

Scalia A. (1989), "The Rule of Law as a Law of Rules," *The University of Chicago Law Review* 56 (4): 1175–1188.

Schoeman D.F. (ed.) (1984), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge.

Sprenger P. (1999), "Sun on Privacy: 'Get Over It'," URL = https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ [Accessed 22.12.2017].

Tamanaha B.Z. (2004), *On the Rule of Law: History, Politics, Theory*, Cambridge University Press, Cambridge.

Tavani H.T., Moor J.H. (2001), "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies," *ACM SIGCAS Computers and Society* 31 (1): 6–11.

Taylor I. (2017), "Data Collection, Counterterrorism and the Right to Privacy," *Politics, Philosophy & Economics* 16 (3): 326–346.

Tréguer, F. (2016), "From deep state illegality to law of the land: The case of internet surveillance in France", URL = https://halshs.archives-ouvertes.fr/halshs-01306332/file/Tr%C3%A9guer%20-%20French%20Intelligence%20Reform%20%28draft%29.pdf [Accessed 25. 11. 2019].

Viseu A., Clement A., Aspinall J. (2004), "Situating Privacy Online: Complex Perceptions and Everyday Practices," *Information, Communication & Society* 7 (1): 92–114.

Vogel E.A., Rose J.P., Roberts L.R. et al. (2014), "Social Comparison, Social Media, and Self-Esteem," *Psychology of Popular Media Culture* 3 (4): 206–222.

Warren S., Brandeis L. (1984), "The Right to Privacy," [in:] F.D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York.

Westin A.F. (1968), "Privacy and Freedom," *Washington and Lee Law Review* 25 (1): 166.

Westin A.F. (2003), "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59 (2): 431–453.

Wolfers A. (1952), "'National Security' as an Ambiguous Symbol," *Political Science Quarterly* 67 (4): 481–502.

Zelikow P. (2003), "The Transformation of National Security: Five Redefinitions," *The National Interest* 71: 17–28.

Zhang H., Shu Y., Cheng P. et al. (2016), "Privacy and Performance Trade-Off in Cyber-Physical Systems," *IEEE Network* 30 (2): 62–66.

Zuboff S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* Pluto Press, New York.