Social Media and National Security: Constitutional Implications of Government Surveillance and Control Measures in India

Sukriti Verma

Dr Rohit K Shukla

Abstract:

In the digital age, social media has emerged as a powerful tool for communication, information dissemination, and community engagement. However, alongside its benefits, social media platforms also present challenges to national security, particularly concerning government surveillance and control measures. This paper explores the constitutional implications of government surveillance and control measures on social media in India. It examines the tension between the government's duty to ensure national security and citizens' rights to privacy and freedom of expression under the Indian Constitution. The paper analyzes relevant legal frameworks, judicial precedents, and emerging issues surrounding social media regulation and its impact on national security. It also discusses the need for a balanced approach that upholds both security imperatives and constitutional rights in the digital era.

Keywords: Social media, National security, Government surveillance, Constitutional implications, India, Privacy, Freedom of expression, Digital rights.

I. Introduction

In India, privacy was declared a fundamental right a few years ago. Since 2013, however, the government has introduced a panoply of digital-surveillance measures, normalising the shift from targeted surveillance to mass surveillance. Attempts to integrate the public and private information of citizens without strong privacy laws and external oversight indicate India’s worrying slide towards a rights-restrictive “surveillance democracy.”

- The emergent surveillance regime involves the state, technological companies, and people themselves, who may collaborate to monitor fellow citizens. While those surveilled are overexposed, the surveillants remain opaque. This increases the chances of rights violations, especially of the traditionally marginalised.

- The functional scope of surveillance has increased with massive digitalisation. It is now part of governance, doubling up as an early-warning system against security threats and a behaviour-moderating system of social management and control.

- New means of surveillance include artificial intelligence (AI)-enabled facial-recognition technology and drones that have been mainstreamed into public life without statutory basis or the consent of the surveilled. Digital surveillance is cost-effective for the state, while increasing harm to the public in cases of biased databases and technological errors.

- COVID-19 has securitised the concept of public-health surveillance by conflating it with public order. This has increased the data burden on private citizens, who can be denied access to public provisions and places if they do not provide their personal information. Without proper safeguards, surveillance can become a tool of exclusion and repression.

Policy Implications

The European Union can hold India, as well as tech companies, to its own strict privacy standards. Data-driven global interactions and digital dependencies necessitate this. To prevent AI products and dual-use surveillance technologies from being used by states against their own citizens, the EU can define and list high-risk ones, deny wide exemptions to states, and incentivise privacy-focused tech. This could help signal a growing global consensus against mass surveillance.

Towards Surveillance Democracy

In early April 2021, as millions of Hindu pilgrims thronged the banks of the Ganges in Haridwar, India, to celebrate the festival of Kumbh Mela, artificial intelligence (AI)-enabled cameras zeroed-in on faces without masks and bodies that violated the physical-distance rule. With corona cases surging past 100,000 per day, surveillance technologies like facial-recognition cameras and drones were meant to convey a sense of security. While the pilgrims were not charged for infractions, invasive surveillance technologies and predictive policing have posed serious threats to individual liberties under the cover of community safety and crowd control.

In the past few years, police in several Indian states have routinised the use of fingerprint- and facial recognition technology (FRT) to stop and screen people on grounds of suspicion. From polling booths to public-transport systems to schools, the use of close-circuit television (CCTV) and FRT on adults and children is turning vital public spaces into privacy-violating zones. In 2019 and 2020/2021, FRT and drones were used on civilians protesting against the contentious Citizenship Amendment Act and farm laws. By scanning, recording, and storing facial and gait data of protesters, the police sought to match their images with mugshot databases (such as voter identity and driving licence) and social media pages. Such technologies tend to have high error rates and are subject to the biases of their human coders (Bailey, Burkell, and Steeves 2020). Faces can be wrongly matched, leading to false arrest. After the 2020 Delhi riots, FRT – with an accuracy rate of 2 per cent or less, as per a 2018 statement of the Delhi Police – was used to recognise over 1,900 people as rioters.

Digital surveillance enables dragnet surveillance, which makes everyone a suspect. This is ethically problematic: people are not just observed but are pinpointed and profiled without their consent.

While this indicates the policing aspect of mass surveillance, the more pervasive issue here relates to the datafication of individuals (turning the identity and activity of human beings into quantifiable data) for governance and business purposes. This exposes individuals to the constant glare of states and private companies. Martin Moore warned in *Democracy Hacked* (2018) of surveillance democracy being a distortion of digital democracy. India faces this prospect. On 16 March 2020, an investigative report revealed that the Narendra Modi government was in the final stages of creating an auto-updating "360-degree database," the Social Registry Information System, to track every aspect of the lives of every Indian (Shrivastava 2020). This would use India's Aadhaar, the world's largest biometric-identity system. There was also a proposal to geo-tag every home. As per media reports, this was to ensure welfare schemes reached their targeted groups.

Trading privacy for better governance or convenience has consequences. Regardless of the subjective prioritising of privacy by individuals, it needs to be valorised as a linchpin right. It affects the rights to speech and expression, to protest, and to not be discriminated against. Digital surveillance is more invasive than traditional surveillance. It can monitor people's activities, associations, locations, emotions, and vital signs. Privacy experts warn against reducing individuals to disembodied data; instead, citizens' data should be treated with the same consideration as their physical well-being (van der Ploeg 2005; Radhakrishnan 2020). This is more so in the age of biometric surveillance, as any data leakage, mistake, or manipulation can lead to bodily harm in terms of denial of an individual's identity and right to access essential provisions. The COVID-19 pandemic has added to this threat by securitising public-health surveillance, making it over-reliant on tech tools.

India, therefore, represents a large digitalising democracy where, in the absence of a data-protection law, digital surveillance by multiple actors is taking diverse forms despite a Supreme Court ruling declaring privacy to be a fundamental right linked with those to life and livelihood (K.S. Puttaswamy v. Union of India 2017). This emergent surveillance regime is hence analysed here. In closing, policy recommendations are offered for the European Union on regulating surveillance technologies and ensuring data privacy for a rapidly changing environment shaped by the pandemic, with the salience of the fourth generation of human rights on digital needs having increased.

II. Historical Context of Social Media in India

Security-Based Mass Surveillance

In 2013, before the former Central Intelligence Agency analyst Edward Snowden exposed government-sponsored mass surveillance programmes like the National Security Agency's (NSA) PRISM in the United States and TEMPORA of Government Communications Headquarters in the United Kingdom, India launched a similar surveillance behemoth: the Central Monitoring System (CMS). Like PRISM, initiated after the attacks of 11 September 2001, the CMS was conceptualised after the attacks in Mumbai of 2008 to aid counterterrorism activities. In tracking terrorist and criminal activities, it got backdoor entry to citizens' data. Strategic surveillance by democracies expanded from international to domestic communications.

The CMS signalled two key changes in old-school surveillance: First, the state announced its move from targeted surveillance of criminals to lawful interception of people's private conversations as per threat perception. Second, surveillance was no longer limited to gathering and storing data. It now involved real-time monitoring of the voice calls, Internet searches, and online activity of potentially anyone with a mobile phone, landline, and Internet connection. Unlike the NSA, which required court approval to spy on calls and emails (though without public scrutiny), the CMS could work without court or even legislative approval. Apart from no external oversight to ensure accountability and prevent the abuse of power, there is no redressal mechanism for individuals whose rights get violated.

This centralised infrastructure of surveillance has hi-tech scaffolding supporting it like the National Intelligence Grid (NATGRID), Network Traffic Analysis (NETRA), and Crime and Criminal Tracking Network Systems (CCTNS). NATGRID, conceptualised as a master database fed by several government departments and ministries, would give intelligence and investigative agencies access to citizens' data including details of bank accounts, telephone records, passports, and vehicle registration. NETRA would automatically intercept voice calls over the Internet if they were red-flagged by keywords like "bomb" and "attack." In 2014, a report based on multiple Right to Information (RTI) appeals revealed that more than 100,000 telephone interception orders were issued by the central government each year (SFLC 2014). This figure could be much higher if orders by various state governments were tallied. The CCTNS is an online tracking system for crimes and criminals linking 14,000 police stations.

This infrastructure has grown. India is set to create the world's largest government-operated facial-recognition database, the Automated Facial Recognition System (AFRS) – with an estimated budget of INR 308 crore (USD 41.62 million; EUR 34.58 million). This would identify anyone from CCTV and video by matching facial biometrics with images from multiple sources. As police often use vague terms like nabbing "suspicious individuals," "habitual protesters," and "rowdy elements" to justify their use of FRT (Bhandari 2021), this could be used to criminalise protest and curb dissent. While civilians first came under security-based surveillance, they were further exposed by governance-based surveillance.

Governance-Based Mass Surveillance

Surveillance as part of governance was brought to the forefront by Aadhaar ("Foundation" in Hindi), as launched in 2009. It provides Indians with a 12-digit unique identity number based on their biometric and demographic data to facilitate access to public goods and services. It received legal backing in 2016, but raised serious privacy concerns when the government started pushing people to link their Aadhaar ID with phone numbers, bank accounts, pensions, and similar – exposing them to the state's disciplinary gaze. This was done by aggregating confidential information about individuals to create their digital duplicate. This made it difficult for people to carry out everyday transactions without having this digital duplicate. For example, a national-election survey conducted by the Delhi-based research organisation CSDS-Lokniti in 2019 showed that due to the linking of ration cards with Aadhaar, a number of respondents from low-income groups were denied food grains either because they did not have an Aadhaar ID or due to technical glitches (Sardesai 2021). Aadhaar was transforming an essential norm of people providing their private information based on "informed consent" to that of now "compelled consent."

In 2018, during Supreme Court hearings, a group of lawyers warned against linking Aadhaar with the National Register of Citizens (to document legal citizens). The Modi government plans to implement this across India. The lawyers feared this could be used for "blacklisting" individuals as non-citizens, denying them access to welfare provisions (Bhatia 2020). Now there is a proposal for a National Digital Health ID, which would store an individual's health-related information. In the absence of a data-privacy law, the state could be privy to the most intimate details of a citizen if this is eventually linked with Aadhaar (Chandran 2020). This could especially affect sexual minorities.

Further, this data could be used for other purposes as this policy allows the state to share anonymised data with third parties. If this health ID is made mandatory, it would mean a denial of certain related services to those who decide to opt out.

Apart from harm by the state, people are vulnerable to external parties in case of data breaches too. In May 2017, for example, India's Centre for Internet and Society pointed out that 130 Aadhaar numbers along with other sensitive data were available on the Internet. Digital surveillance, while expanding the powers of states to surveil, has also brought on board private actors with even greater capacities to grab mass data. Social media platforms emerged as data-rich sites of surveillance.

Social Media Surveillance

Canadian political-communications expert Vincent Mosco (2014: 10) spoke of a surveillance state reinforced by "surveillance capitalism" (companies using big-data analytics to track and target users for profit). In the EU, the scale of this tracking is reduced due to the General Data Protection Regulation 2016/69 (GDPR). In India, tech platforms can easily surveil users. India has not enacted its Data (Privacy and Protection) Bill 2017 and Personal Data and Information Privacy Code Bill 2019 (modelled after the GDPR). The latter, in its current form, gives wide exemptions to the government in accessing people's sensitive personal data.

Freedom House's "Freedom on the Net 2019" reported that governments are increasingly relying on social media to spy on their citizens. In 2019, Facebook in its "Transparency Report" stated that India was second only to the US in requesting the company provide users' data; it had complied in 53 per cent of cases. In 2020, two years after the Supreme Court stopped the government from creating a Social Media Communication Hub to monitor the social media accounts of citizens, the Modi administration started planning for a surveillance tool to monitor individual users. Forty government departments already have access to a social media surveillance tool called Advanced Application for Social Media Analytics (AASMA) to collect live data of users from multiple social networks, do sentiment analysis on the content they post, track their location, and alert authorities accordingly.

With social media, surveillance functions and laws evolved – from the interception of voice calls by the Indian Telegraph Act (1887) to interception of digital communications by the Information Technology Act/IT Act (2000, 2008) to monitoring online media content by the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021). The state could legally monitor digital content on any device or platform and prosecute anyone for vaguely stated offences like threats to the sovereignty, integrity, or security of India or having friendly relations with foreign states. Arresting people for satire or criticism of the government is a new form of repression. Several states in India have misused the IT Act to arrest people for social media posts (Section 66A of the Act) and to block/takedown web pages and accounts (Section 69A of the Act). The fact that social media was now a space of surveillance had a chilling effect on self-expression. The Supreme Court repealed Section 66A in 2015, but the police still use it to make unconstitutional arrests regardless.

Social media surveillance adopts the tactic of "content moderation." On 12 February 2021, during the farmers' protests, Twitter blocked 97 per cent of the accounts the Modi government ordered it to. These accounts had been highly critical of the government. The online space, projected as the stronghold of free speech, was further gagged by the IT Rules passed on 25 February 2021. The government could now decide which social media posts, streaming shows, and digital news could be taken down. Even the final frontier of privacy – encrypted services like WhatsApp – has come under the state's scrutiny. In the past five years, WhatsApp claims to have securely delivered over 100 trillion messages to over two billion users globally, with India being its largest market. The government could ask companies to break their own privacy-respecting encryption.

Industry Support

Private companies are equipping the state with new means of surveillance. The "Spy Files" project of the whistle-blower website Wikileaks revealed Indian companies to be in the top league of the global surveillance industry. With law enforcement and military agencies as their major clients, Indian companies have been innovating on facial- and fingerprint recognition, predictive intel, decryptors, and, now, COVID-19 tech for homeland security.

Companies like FaceTagr and StaqU provide FRT and AI solutions to police. Mobineer Info Systems is building a smart-policing app called E-Beat Book for foot-patrol police that would include FRT to match people's faces with databases and obtain information on them rapidly. Kommlabs Dezign sells interception solutions that reveal what people sound and feel like, and not just what they say. They have AI-enabled solutions to detect cognitive and emotional stress in voice calls. Like FRT, Emotion Recognition Technology is the sunrise sector of the surveillance industry. It is highly controversial, as biases are baked into the system. This can lead to a future where someone is arrested because they sound guilty. India is also among the leading countries in CCTV surveillance. Videonetics helps in video surveillance. Shoghi Communications provides surveillance tech to national-security agencies. ClearTrail and Comtrail provide tech for the interception and monitoring of voice and internet data. Foreign companies like, among others, China’s ZTE, Japan’s NEC, the US’s Verint Systems, and Germany’s FinFisher and Utimaco add to this arsenal.

Lateral Surveillance

The state’s power to surveil people for security and governance, boosted by tech and private companies, has another supportive actor: people themselves. In February 2021, the Ministry of Home Affairs launched a controversial programme inviting private citizens to report on unlawful activities on the Internet and social media. The Indian Cyber Crime Coordination Centre (14C) invited citizens to become Cyber Volunteer Unlawful Content Flaggers, Cyber Awareness Promoters, and Cyber Experts. The fear is that citizens who support the ruling party can easily volunteer as Content Flaggers to muzzle critics and dissenters and get them arrested, similar to China’s community monitors under its grid-management system of granular surveillance. This fear is real: a database on sedition cases compiled by Article 14, an Indian news and investigations site, revealed that 96 per cent of those filed against 405 individuals for criticising politicians and governments over the last decade were registered after the Modi government came to power in 2014 (Purohit 2021). Human Rights Watch in its “World Report 2020” also documented the growing arrest of critics and opponents of ruling political parties both at the centre and in some states. These cases were often filed by partisan supporters.

Another variation of this surveillance has been vicious trolling as well as threat of arrests for online content the public supporters of the ruling party describe as being anti-Indian or hurting religious sentiments (Ellis-Petersen 2020). Societal distrust grows as people censor one another. Citizens are no longer community-level watchers and reporters. Instead, they are arrogating to themselves policing powers (Swaminathan and Saluja 2021).

Pandemic Surveillance

The pandemic has encouraged citizen vigilantism powered by the rationale of public health. In 2020, there were cases of Residents Welfare Associations (self-administering bodies in housing complexes and colonies) in the northern cities of Noida and Gurugram forcing residents, visitors, domestic workers, and other service providers to use the government’s contact-tracing app Aarogya Setu (“Bridge of Health” in Hindi). They acted as extensions of the state. The government would make the app mandatory for travel to public or private workplaces and by train, subway, and airplane.

This represents a new normal of surveillance: people were now asked to wear or carry the means of their own surveillance. This body-tagged (wearable devices) and geo-tagged (smart device-based pandemic trackers) surveillance is not limited to identifying and isolating infected individuals, but fining and arresting them in case of lockdown or quarantine violations. There are currently 120 contact-tracing apps across 71 countries in existence. As per the COVID-19 Digital Rights Tracker, Aarogya Setu is the most downloaded among them (with more than 100 million users). It has privacy issues, as it is seeded with people’s personal details. It uses static identifier (reducing potential for anonymity), and collects more information than required – thus violating the “purpose limitation” (data collected for a specific purpose and not used for other ones), “data minimisation” (basic amount of data collected to fulfil a specific purpose), legality, and proportionality requirements of India’s privacy ruling of 2017 and the GDPR (Internet Freedom Foundation 2021). On 30 March 2021, an RTI document by lawyer Saurav Das revealed that the Jammu and Kashmir administration had shared the app’s data about people’s health with the police, violating purpose limitation.

Sensitive health data needs the highest level of protection. Aarogya Setu, however, does not hold the government liable for violations of data privacy. It also demonstrates the pitfalls of techno-solutionism, as it is not error-proof. There have been incidences of false negatives and false positives. India, like 21 other countries including Australia, France, and the US, is using drones to surveil people and enforce COVID-19 measures. Drones capture body and location data, and are not bound by privacy clauses. This has generated deep-seated fear among the surveilled, increasing the stigmatisation and targeting of already-vulnerable groups like women, Muslims, daily **wage earners, gig workers, and the transgender community (Radhakrishnan 2020).**

III. Government Surveillance and Control Measures

For a long time, large-scale government surveillance was a hallmark of authoritarianism. Authoritarian states known for their extensive surveillance systems include the GDR, the People's Republic of China, the Soviet Union, and North Korea.[1] In the past few decades, however, established liberal democracies have been increasingly ready to monitor their citizens on a massive scale. One notorious surveillance program run by an alliance of democracies was uncovered by Edward Snowden. The current rise of large-scale government surveillance is widely viewed with great concern, if not outright horror. Critics fear the rise of Orwellian surveillance states and celebrate Edward Snowden as a paragon of civil disobedience.[2] Much of the criticism of government surveillance has revolved around privacy, its meaning and value, and how it is impacted by surveillance. Government surveillance and the erosion of privacy it is associated with are being discussed as a cause of distrust and feelings of vulnerability, as a potential source of discrimination and unjust domination, and as a threat to democracy and the integrity of the public sphere, to name but a few concerns. By many, existing government surveillance programs are also deemed disproportionate.[3]

At the same time, there remains some ambiguity about the acceptability of surveillance in democracies. For one thing, recent technological advances have made large-scale government surveillance not only feasible and cheap but also, in one sense, less intrusive. Modern government surveillance relies increasingly on technology rather than human spies and informers. Surveillance practices include, for instance, the monitoring of public spaces with CCTV cameras, the automatic interception and retention of Internet and telecommunication traffic, and the use of artificial intelligence to make sense of the huge amounts of data collected. As a result, modern surveillance is characterized by the rarity of actual human access to the large quantities of data collected. While the quantity of data collected is staggering, only a small proportion of them are ever accessed by a human person. Human access to collected surveillance data can be expected to further decrease as artificial intelligence becomes more sophisticated. This has led to a debate about whether modern surveillance even reduces the privacy of those subject to surveillance, with some arguing that modern surveillance, involving little human access to the collected data, tends to leave people's privacy intact.[4]

For another thing, surveillance operations by democracies seem much more acceptable than the kind of surveillance conducted by authoritarian regimes. Democracies are using surveillance mostly for seemingly innocuous purposes, such as combating terrorism and serious crime or, most recently, containing the spread of a deadly virus. They are less inclined to use surveillance to crush legitimate political opposition or to persecute members of stigmatized groups,

[1] For an overview of policing and surveillance in twentieth-century dictatorships, refer to Dunnage (2016). Dunnage reports that it is estimated that, in the post-Stalinist Soviet Union, some 30 to 60% of the population were forced to work as informers for the KGB, and in the GDR, roughly every thirtieth citizen served as an informer for the regime. Nazi Germany may have relied less on surveillance and more on denunciations (pp. 122–123). On surveillance in China and North Korea, see Denyer (2018) and Lankov and In-ok (2011), respectively.

[2] See, e.g., Brownlee (2016) and Scheuermann (2014).

[3] Critical discussions of government surveillance include Goold (2009); Henschke (2017, ch. 9); Hoye and Monaghan (2018); Lever (2008); Nissenbaum (1998); Roberts (2015); Solove (2007); Smith (2020); Stahl (2016, 2020); and I. Taylor (2017). For two non-privacy-centered criticisms of government surveillance, see Macnish (2018, 2020) and Sorell (2018). A classic treatment of this topic is Foucault (1975). See also Zuboff (2019), though her focus is on "surveillance" by private companies.

[4] Most prominently Macnish (2018, 2020); see also Posner (2005) and Sorell (2018). For an argument that public video surveillance does not violate privacy rights, refer to Ryberg (2007).

notable exceptions notwithstanding.[5] There is a significant moral difference, then, between, say, the NSA and the East German *Stasi*.[6]

In sum, when democratic governments conduct large-scale surveillance operations in the pursuit of seemingly innocuous goals, all while limiting human access to the collected data, the case against surveillance is at least not obvious. In fact, some philosophers have expressed wholehearted support for large-scale government surveillance. Noting that it is generally permissible for law enforcement agencies to secure information about past events, one advocate of government surveillance has suggested that “the State should place all of its citizens under surveillance at all times and in all places.”[7] Others have invoked catastrophic risks, such as those posed by biological and nuclear weapons of mass destruction, to justify extensive government surveillance.[8] To be sure, such wholesale endorsements of government surveillance are the exception.[9] But they convey an idea of the ethical ambivalence of government surveillance.

My goal in this paper is to contribute a new perspective on what is ethically at stake when democratic governments monitor their citizens and to achieve a better understanding of what is pro tanto objectionable about it.[10] I will proceed by distinguishing three independent concerns that a critic of government surveillance may have. The first concern is that governments diminish citizens’ privacy by collecting large amounts of data. This concern focuses on the loss of privacy brought about by the collection of data as such, that is, irrespective of whether the data will be accessed or used for objectionable purposes. The second concern is that the collected data may be accessed after all, again causing a loss of privacy, though of a different kind. The data may be accessed by government employees or exposed to the public through a hack or a leak. The third concern is that the collected data may be used for objectionable purposes (other than accessing the data).

Two of the above introduced concerns revolve around privacy. Zooming in on these two concerns, this paper seeks, first, to shed light on the significance of privacy in the context of surveillance. Engaging with the debate about the meaning of privacy, I will suggest that, whereas access to data is objectionable as such, the privacy loss brought about by the mere collection of data does not constitute an independent reason to object to government surveillance. Second, moving on to the third concern, the paper seeks to achieve a better understanding of problems associated with what surveillance can be used for. I will suggest that one serious and underappreciated problem with surveillance is related to the problem of political legitimacy. Surveillance can be used to enforce laws that lack legitimacy.

My discussions of privacy and legitimacy, though motivated by concerns about government surveillance, are, I hope, of more general relevance and thus of interest to scholars who have no particular interest in surveillance.

Surveillance and Privacy

I want to begin by examining the first concern about privacy, that is, the notion that there is something objectionable about government surveillance because the collection of massive amounts of data reduces people’s privacy. By undermining people’s privacy, government surveillance may be deemed objectionable irrespective of whether the data are accessed (second concern) or used for objectionable purposes (third concern). It is, in this sense, an *independent* concern about government surveillance.

There are four reasons why this concern is worth looking at. To begin with, it is a very natural thought that surveillance is objectionable simply on the grounds that the collection of people’s data reduces their privacy. Privacy is a widely valued good, and the mere collection of data is thought by many (though not all) to undermine privacy. It is therefore

[5] Exceptions include surveillance in the McCarthy era, the FBI’s COINTELPRO (including the wiretapping of Martin Luther King), and undercover policing in the UK (see the ongoing Undercover Policing Inquiry). See also Goold (2009, p. 43).

[6] See Sorell (2011, pp. 12–14).

[7] J. S. Taylor (2005, p. 227).

[8] Persson and Savulescu (2012)

[9] Much more cautious defenses of surveillance have been advanced by Smith (2020) and I. Taylor (2017).

[10] In what follows, the “pro tanto” will usually be omitted, but I will return to it in the conclusion.

natural to object to the collection of data simply on the grounds that this violates people's privacy — irrespective of whether the other two concerns apply.

Moreover, the extent to which increasingly automated surveillance practices really involve privacy losses is, as already noted, intensely discussed among privacy and surveillance scholars. An underlying assumption here seems to be that if the collection of citizens' data reduces their privacy, surveillance is ipso facto problematic, irrespective of whether the data will be accessed or used for malicious purposes. Why else think that it matters how we define privacy and whether it is undermined by surveillance? Surveillance may be thought to be problematic simply in virtue of the fact that it undermines people's privacy.

Yet another reason why the validity of the first concern matters is that some might question the force of the other two concerns. Human access to the collected data is very limited, and established liberal democracies may seem to use surveillance mainly for justifiable purposes. In light of this, some might question why we should object to large-scale government surveillance at all. If there is something objectionable about collecting large amounts of data as such (because of the privacy breaches associated with it), the critic of government surveillance has a ready answer to this question.[11]

Finally, discussing this first concern will contribute towards achieving the overarching goal of this paper, namely a better understanding of how surveillance and privacy concerns relate to each other and how the potential harm done by government surveillance should be characterized. I believe that the first concern is ill-founded in that it fails to constitute a compelling independent reason to object to government surveillance, over and above the other two concerns. Appreciating why this is so allows a better understanding of the problem of government surveillance and of what is at stake in debates about the meaning and value of privacy.

Notice first, then, that the idea that there is something objectionable about the collection of data as such, though natural, can be challenged by means of a thought experiment. Imagine an unrealistically benevolent, well-organized, and stable democratic state that engages in large-scale surveillance operations. The state is characterized by the following two features:

1. Thanks to excellent institutional safeguards and security measures, there is no risk that data is illicitly accessed by government employees, nor that data might be exposed to the public.

2. It uses the collected surveillance data to enforce laws in a legitimate and just manner. It never uses the surveillance capacities for objectionable purposes. It also boasts a set of unrealistically robust checks and balances, which completely remove any risk of the surveillance capacities being used for less benign purposes in the future.

Admittedly, such perfectly benign surveillance is difficult to imagine. But when we do imagine it, it is difficult to see what might be objectionable about it. Once we stipulate that there is no risk of illicit access to the collected data and that the surveillance capacities will only ever be used for good purposes, that is, once we stipulate that the other two concerns do not apply, there just seems little cause for concern. On the contrary, it is arguable that we should welcome such perfectly benign surveillance. It provides enhanced security without any obvious downsides. To object to such perfectly benign surveillance would, it seems to me, be quite irrational. To be sure, we may have a residual feeling of unease at the thought even of such benevolent large-scale government surveillance (I, for one, certainly feel uneasy at the thought of it). But this is probably because no surveillance system in the real world resembles this perfectly benign surveillance system. Our emotional responses have been trained on a data set of surveillance practices that invariably do not meet the above two criteria. Upon rational reflection, we should welcome surveillance of this sort.

This provides at least initial grounds for thinking that the first concern must be ill-founded. The collection of large amounts of data as such — divorced from the other two concerns — seems unobjectionable. But one might still find

[11] The observation that no access takes place when data are processed by intelligent algorithms might be challenged on the grounds that these algorithms are themselves "agents" of sorts, who "access" the data when processing them. Whether intelligent systems qualify as "agents" or not, I agree with Macnish (2020) that there is a significant difference between access by humans and access by entities that lack "semantic understanding," e.g., intelligent systems.

the above line of reasoning unconvincing as it entirely brackets the key issue of privacy. Indeed, I have made two seemingly conflicting claims. On the one hand, I have just suggested that there does not seem to be anything problematic about the collection of data as such, divorced from the other two concerns. On the other hand, I have suggested that the collection of large amounts of data may diminish citizens' privacy. This raises the question how the collection of large amounts of data could possibly diminish people's privacy without being in any way problematic as such. If it diminishes their privacy, does this not show precisely that there is something objectionable about surveillance irrespective of whether the data are exposed or used for objectionable purposes?

To resolve this tension, and more generally to understand how surveillance and privacy relate, it is useful to briefly consider the debate about the meaning of privacy. One view in the literature is that privacy should be spelled out in terms of control. A person's privacy remains intact as long as this person retains control over her personal information.[12] Beate Rössler, for instance, proposes the following definition: "Something counts as private if one can oneself control the access to this 'something.'"[13] On this view, privacy is reduced as soon as one loses the relevant sort of control. A competing view holds that privacy is a matter of access, not of control. A person's privacy is intact to the extent that no one actually accesses her personal information. Mere loss of control over one's personal information is not enough for there to be a reduction of privacy. Kevin Macnish has made the case for the access account by appeal to the so-called threatened loss cases. Threatened loss cases are characterized by a loss of control over one's personal information in the absence of actual access to it. He invites us to consider the case of a person who left her diary on a table in a coffee shop. When she returns to the coffee shop to pick it up, it is handed back to her by a stranger in whose possession it was for the last 30 minutes. During this interval, the diary owner had lost control over her personal information in the diary. But if the stranger did not open the diary during this time, it seems plausible that the diary owner's privacy has not been comprised. Such threatened loss cases suggest that what matters is actual access rather than loss of control.[14]

IV. Constitutional Implications of Government Surveillance

An assumption underlying this debate is that there is a lot at stake in the dispute about the meaning of privacy. Recall that modern government surveillance, relying increasingly on technology rather than people, involves relatively little actual human access to the collected data. Depending, then, on how we define privacy, modern government surveillance involves either privacy erosions on a massive scale (control account) or hardly any privacy losses at all (access account), given that it involves loss of control over one's personal data but little actual human access to them.[15] This is why how we define privacy has been taken to matter a great deal.

Notwithstanding the many valuable insights this debate has generated, I do not believe that how we define privacy matters as much as is commonly thought. Little of substance depends on it. Whether we should think of government surveillance operations as reducing privacy in the strict sense of the term or not is, at the end of day, not that relevant. Indeed, Macnish himself, who in the title of a paper asserts that "defining privacy matters," is (rightly, I think) adamant that government surveillance is problematic even if, technically, citizens' privacy is not diminished.[16] This begs the question why exactly it should matter which definition of privacy we opt for. I believe it does not matter all that much.

[12] I am focusing on informational privacy, as this seems to be the relevant kind of privacy in the present context.

[13] Roessler (2005, p. 8). Other proponents of the control account include Fried (1984, p. 209); Menges (2020a); Moore (2003, 2008); Westin (1967, p. 7); and, tentatively, Mainz and Uhrenfeldt (2021) (the latter focus on the right to privacy, though). For an interesting exchange about its plausibility, see Lundgren (2020) and Menges (2020b).

[14] Macnish (2018); see also Macnish (2020) and Thomson (1975, pp. 304–305, n. 1). An argument strikingly similar to Macnish's (that even features a diary example) was independently developed by Tom Sorell (2018). For a subtle attempt by a control theorist to account for threatened loss cases, refer to Menges (2020a, forthcoming).

[15] Note, though, that Menges, although a control theorist, tries to capture the intuition that no privacy loss occurs in threatened loss cases and thus agrees with Macnish that modern government surveillance involves very little loss of privacy (2020a, 2020b, forthcoming).

[16] Macnish (2018, 2020). Menges concurs (2020a, pp. 46–47). A view similar to Macnish's has been defended by Sorell, who "den[ies] that bulk collection is seriously intrusive without denying that it is morally objectionable in other ways" (2018, p. 47).

What matters are the actual wrongs and dangers of surveillance, and their exploration does not require resolving the dispute between access theorists and control theorists.[17]

I therefore wish to sidestep this debate by engaging in an act of conceptual stipulation. I suggest that we distinguish *two* concepts of privacy: "access privacy" and "control privacy." Access privacy is the kind of privacy that requires nonaccess to one's personal information, whereas control privacy is reduced as soon as one loses control over one's personal information, whether accessed or not. Modern government surveillance, to the extent that it does not involve human access to the collected data, reduces control privacy while leaving access privacy mostly intact.[18] The suggested distinction is a technical stipulation. By making this stipulation, I am not suggesting that our everyday concept of privacy is fundamentally vague or ambiguous. Perhaps it is, but I am not committed to this view.[19] Nor do I mean it to discourage further inquiry into how to best analyze everyday privacy talk, which strikes me as an interesting undertaking in its own right. But introducing these two technical concepts by means of stipulation allows us to sidestep an intricate and unresolved debate, and it yields two technical concepts that are useful for analytical purposes. To be sure, the proposed terminological stipulation tells us little of substance about the significance of privacy in the context of government surveillance. But it helps us organize our thoughts and get more quickly to the heart of what is normatively at stake.[20]

V. Conclusion

Having distinguished three potential reasons for concern, I have argued that, ultimately, we ought to be concerned about whether collected surveillance data may be accessed and about what the data are used for. The mere collecting of surveillance data, though involving privacy losses of sorts, does not constitute a compelling reason for concern in its own right, over and above the other two concerns. Debates about the meaning of privacy, though insightful, need not be settled for the ethical assessment of government surveillance. One chief problem with government surveillance in democracies is that it may be used to enforce laws that ought not to be enforced — a problem that will become increasingly acute as government surveillance expands.

I conclude with a caveat regarding the implications of my argument. The aim of this essay was to get a better grip on what is pro tanto objectionable about modern government surveillance in established liberal democracies. I have made no attempt to provide an all-things-considered judgment of its ethical acceptability. Nothing I have said entails that government surveillance is never justified. To call for an end to all government surveillance on the basis of the above

[17] I am here concurring with Henschke (2017, p. 46), Solove (2007, p. 760; 2009, pp. 39–40), and van den Hoven (2008), who have warned against getting bogged down in conceptual debates.

[18] Henschke (2020), too, suggests distinguishing two concepts of privacy. His distinction differs from mine. In his 2017, he defends a pluralistic, "clustered" approach to privacy.

[19] For what it is worth, I share Macnish's linguistic intuition that privacy is only reduced in situations in which human access occurs.

[20] An anonymous reviewer has sensibly suggested that I clarify whether this approach commits me to the views that (1) defining privacy is not crucial to assessing the ethical permissibility of surveillance, and (2) intermediate moral principles such as "Do not diminish a person's privacy [or, for that matter, autonomy, freedom, etc.]" play little role in moral theory compared to more fundamental principles such as the categorical imperative or the utilitarian calculus. In response, I wish to state that I do believe that defining privacy matters, and I have offered two stipulative definitions of privacy. What I do not believe is that we necessarily need to determine which of several privacy definitions on offer (especially privacy as control and privacy as nonaccess) best capture everyday privacy talk before we can address the ethical issue at stake. We can proceed by exploring both the normative significance of reductions of control privacy and that of reductions of access privacy. This way, we can come to grips with the problem of surveillance without first having to identify which concept of privacy best captures everyday privacy talk. This is the approach I am taking in this essay. Relatedly, I am not committed to the view that intermediate principles do not matter for moral theorizing. Such principles as "Do not diminish a person's privacy" do play a role in moral theorizing, but again, we can work with different versions of such principles (e.g., "Do not diminish a person's control privacy," "Do not diminish a person's control privacy," etc.), and we need not first identify which privacy concept best captures everyday privacy talk.

concerns, perhaps by appeal to the precautionary principle, would be to ignore the opportunity costs that forgoing government surveillance may involve.[21] As mentioned in the introduction, some scholars have defended government surveillance as a useful instrument for preventing terrorist attacks of a catastrophic scale. An all-things-considered judgment that accounts for these and other potential opportunity costs, which would also require assessing the actual effectiveness of surveillance, cannot be provided within the scope of one article.[22] Indeed, it is doubtful that any such general assessment can be provided, as the moral costs and benefits of each surveillance technique or operation must be judged on its own terms.[23] What I do hope to have achieved is to contribute a new perspective on whether and why we should be concerned about government surveillance and on how the problem of government surveillance relates to questions of privacy and legitimacy.

[21] See Sunstein (2005).

[22] On the questionable effectiveness of the NSA's surveillance program, see Greenwald (2014, pp. 202–205). Refer to Macnish (2015), Rønn and Lippert-Rasmussen (2020), and Thomsen (2020b) for discussions of government surveillance and proportionality, which may be helpful for reaching more comprehensive judgments.

[23] For one moral assessment of a specific surveillance practice, see Thomsen (2020a).