The legacy of the privacy versus security narrative in the ECtHR's jurisprudence

VB verfassungsblog.de/os6-privacy-vs-security/

Eliza Watt

This article belongs to the project » 9/11, zwei Jahrzehnte später: eine verfassungsrechtliche Spurensuche
This article belongs to the debate » 9/11 und die Privatsphäre
21 April 2022

In this post I trace the modern culture of mass surveillance to the UN policy of counterterrorism resulting from the 9/11 attacks on the United States. I argue that balancing security needs with privacy rights on the basis of the traditional security/privacy trade-off is misguided, and identify the complexities involved in the modern culture of surveillance. Further, I highlight that the security narrative has always played an important role in the European Court of Human Rights' (ECtHR) law making, ultimately leading to the Court's embracing of mass surveillance practices.

Privacy vs Security: The Misguided Trade-off

One of the inevitable consequences of the 9/11 UN counterterrorism policy is a 'surveillance industrial complex' fuelled by heightened threat narrative, initially presented by some governments as a trade-off. Accordingly, security can only be achieved if it is accepted that states must conduct mass surveillance in order to keep their citizens safe. While this means sacrificing their fundamental rights-the argument goes-this is the price to be paid for attaining greater safety for all. Most importantly this means compromising the right to privacy, being 'the presumption that individuals should have an area of autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals'.

The two decades of counterterrorism strategy that followed attest to the fact that the security/privacy trade-off approach is not only outdated, but it also amounts to a gross oversimplification of the complexities involved in the modern culture of surveillance. First, it has been contended that the threat of terrorism has at times been sensationalized owing to deliberately engineered 'politics of fear'. This arguably resulted in the UN prioritising, magnifying and overestimating terror-related risks over other existential threats to international peace and security, thus consequently diverting resources and attention from other pressing issues, such as climate change or deadly pandemics. To illustrate this, in statistical terms the estimated number of deaths in 2021 from the Covid-19 pandemic was reported to reach 1,884,146 compared with 7, 142 deaths recorded due to global terrorism. Secondly, the traditionally defined trade-off discounts the 'public-private symbiosis', which sees data as a commodity to be exploited for commercial gains

through state-business partnerships. It follows that spying and surveillance can no longer be perceived as purely pursued for political or economic ends between nation states or explained solely as a national security necessity. Commercial spying, known as 'surveillance capitalism', by private companies in the form of consistent monitoring, predicting and influencing consumer behaviour on the Internet is now habitually carried out for profit and often merges and collaborates with state surveillance, forming a global 'surveillance industry'.

One example being the 2021 Pegasus scandal, software sold worldwide by the Israeli NSO Group to governments, including within the European Union (EU), to spy on a coterie of world leaders, politicians, human rights activists and journalists rationalised inter alia by the need to fight terrorism. As Amnesty International put it, this case is emblematic of the private sector facilitating surveillance, of impunity of states and companies in deploying it, together with the failure of the former to fulfil their obligations to protect individuals from unlawful hacking and surveillance.

Of equal importance in this emergent paradigm is the role of individuals, who often voluntarily surrender their privacy by publicly sharing their data on social media platforms such as Instagram, YouTube, or Twitter. This phenomenon is termed 'participatory panopticon' and described as 'constant surveillance [which] is done by citizens themselves, and [which] is done by choice'. For these reasons alone, presenting the problem of reconciling security needs with privacy rights as a 'trade-off' is misplaced. Democracies depend on data as a commodity and spying related to national security apparatus is but one manifestation of new culture of persistent surveillance, which is here to stay. Rather than a trade-off, it must be redefined in terms of cost-benefit analysis. This means the estimate of the real cost to privacy and related human rights associated with mass surveillance whilst not attaining security to the degree advocated by governments, and fully recognizing the resultant commercial gains made by governments and the private sector alike.

ECtHR Jurisprudence on Mass Surveillance post Snowden Disclosures

The post-9/11 culture of mass surveillance has been subject to extensive and fierce debate, especially in the years that followed the revelations made by Edward Snowden in 2013. Strict legal scrutiny, in particular by the European Court of Human Rights, has played a significant role in this discourse. This is because in its mass surveillance case law the Court addresses states' arbitrary interference with the right to privacy set out in Article 8 of the European Convention of Human Rights (ECHR), which national authorities have often justified on national security/terrorism grounds.

In a number of important cases, including *Roman Zakharov v Russia*, *Centrum för Rättvisa v Sweden* and *Big Brother Watch and Others v United Kingdom*, the ECtHR has remarkably adjusted its jurisprudence, in some instances rejecting well settled principles upon which it had previously relied. Two issues vividly illustrate this unprecedented

transformation, namely the Court's approach to the right to bring an individual complaint (the so-called 'victim status') and its acceptance of mass surveillance programmes *per se*.

The Right to Bring a Claim Before the ECtHR in Surveillance Cases

Under Article 34 of the ECHR, the ECtHR may hear applications from an individual, non-governmental organization or a group claiming to be a victim of a violation of any of the ECHR rights by any of its contracting state parties. For the best part of six decades, the Court consistently interpreted this provision as requiring from the applicant to evidence that he or she was personally and directly a victim of violation and, more recently, that he/she suffered a 'significant disadvantage'. If these criteria were not satisfied, the Court would not review the member state's law or policy *in abstracto*, that is in the absence of any evidence as to how his/her privacy was actually violated. This changed significantly in 2015 as a result of *Zakharov v Russia*. In this case the Court recognized that individuals would not normally be aware of being the subject of secret surveillance and allowed cases to be brought even where the claimant cannot prove that they were the subject of a concrete surveillance measure. By allowing an individual to claim to be a victim of a state's violation on the basis of the mere existence of secret surveillance methods, or of legislation permitting their operation provided that he/she can show to potentially be at risk of being subjected to them, the ECtHR was able to scrutinise state clandestine surveillance in Europe ever since.

The key outcomes of this striking change are the landmark cases of *Big Brother Watch* and *Centrum för Rättvisa,* issued in parallel, both concerning bulk interception of foreign communications by the United Kingdom and Sweden respectively. For two reasons the judgements are of vital importance for the future of Council of Europe (CoE) states' spying policies. First, the ECtHR has explicitly recognized mass surveillance regimes as not *ipso jure* incompatible with Convention rights. In contrast, the Court of Justice of the European Union (CJEU) in a number of high profile cases held that blanket retention and data sharing arrangements with third countries are incompatible with the EU citizens' rights to privacy and data protection. The CJEU reaffirmed this stance in early April 2022 in *Commissioner of An Garda Síochána and Others*. It held that as a general principle, EU law does not allow for legislation that as a preventative measure permits general and indiscriminate retention of traffic and location data for the purposes of combating serious crime, but it does not preclude member states' targeted and time limited legislative data retention measures.

Secondly, the ECtHR recognized the challenges states face with fighting serious crime and international terrorism brought about by the changes in technology and communications. It therefore updated the procedural safeguards for secret surveillance that states must put in place to comply with the ECHR. Under Article 8(2) of the ECHR an interference with privacy rights can only be justified if it is in accordance with the law, pursues one or more of legitimate aims and is necessary in a democratic society to achieve those aims.

ECtHR Embracing of Mass Surveillance Regimes in Europe

States' safeguarding national security against acts of terrorism have long been accepted by the Court as a legitimate aim. In *Weber and Saravia v Germany* and *Liberty v United Kingdom* the ECtHR expressly recognized that national authorities enjoy a wide margin of appreciation in choosing how best to achieve national security, thereby acknowledging that bulk interception regimes do not *per se* fall outside this margin. In *Big Brother Watch*, the Court also confirmed that such measures are a lawful means for states to gather foreign intelligence, for early detection and investigation of cyberattacks, counter-espionage and counterterrorism. In doing so, the ECtHR endorsed the utility of bulk interception tools, considering these as 'a valuable technological capacity to identify new threats in the digital domain'. Yet, serious doubts have been raised on numerous occasions regarding the true effectiveness and therefore the necessity and proportionality of this practice. This is evidenced by steady increase in global terrorist attacks since 9/11, whilst attesting to the unnecessary sacrifices of individual privacy and damage to foreign relations that they cause.

As a result of these judgements and the concomitant normalisation of mass surveillance , the ECtHR was criticised for fundamentally altering the existing balance in Europe between the right to respect for private life and public security interests. Further, instead of outlawing bulk regimes altogether, the Court focused on establishing new procedural standards, termed as 'end-to-end safeguards', that must be present at every stage of operations (i.e. throughout the entirety of the intelligence cycle) and set out new criteria specifically for bulk surveillance schemes that domestic law must specify. It thereby signalled that states operating such surveillance regimes will be scrutinised henceforth against this benchmark.

New Procedural Safeguards for Bulk Interception of Foreign Communications

This approach may be viewed as problematic for at least two reasons. First, under Article 35 of the ECHR, the ECtHR will deal with the matter at hand only after all domestic remedies have been exhausted unless these are ineffective or their alleged ineffectiveness is the main contention made by the applicant. Since secret surveillance cases are decided *in abstacto* and given the Court's focus on procedural compliance of bulk surveillance regimes with the new safeguards established in the *Big Brother Watch* case, the ECtHR may be at the brink of pursuing a new trajectory, and becoming the equivalent of a European Constitutional Court for privacy cases. Indeed, rather than scrutinising concrete violations of Convention rights and the need for a remedy by the victim, the Court has agreed to review surveillance laws in general thus assuming the role of the court of first instance at a national level and requiring the legislator to revise or amend the law in question when the Court considers it necessary. This, it has been suggested, marks a shift towards the ECtHR scrutinising the Convention states' legislative branches' respect for the rule of law and the basic requirements of law making.

Secondly, the Court is prepared to hold violation of Article 8 rights far more willingly when it comes to states' domestic secret surveillance, compared to bulk intercepts of foreign communications, as attested by the *Zakharov* case and most recently in *Ekimdzhiev and Others v Bulgaria*. Here the ECtHR found that the Bulgarian law permitting secret surveillance, access and retention of communications of practically everyone in that country breached the right to privacy, as the law did not meet the 'quality of the law' criteria. This is inter alia because parts of that law were insufficiently clear, the independence of the oversight body could not be guaranteed, whilst both the notification procedures and the remedies were ineffective. Consequently, the Court concluded that the Bulgarian law was incapable of keeping the surveillance to only that, which is necessary. The case sends a strong message to the CoE states: In a democracy secret surveillance powers must not be abused and governments must provide adequate, sufficient supervision and approval to protect against abuse, together with the right to be informed. The question nevertheless remains as to how to reconcile the Court's apparent embracing of bulk interception of foreign communications so long as it adheres to the procedural guarantees, with its continued antagonism towards domestic secret surveillance methods.

The ECtHR's Continued Reliance on the Security/Privacy Trade-off Narrative

The ECtHR acceptance of bulk interception regimes as measures that in principle fall within states' discretion in fighting international terrorism seems to be predicated on the traditionally conceived privacy/security trade-off. Although the Court adopted a lenient approach to the issue of the 'victim status' in surveillance cases, it has also shown to readily succumb to the security narrative. This is because it explicitly recognized the value of mass surveillance methods for security operations by supporting the CoE states' intelligence services pro-active approach in relation to unknown threats emanating from abroad. By doing so the Court is at the risk of discounting the complexities involved in the modern industry of mass surveillance, including the rationale for conducting it, the parties involved and the technical means at the disposal of state and non-state actors. Viewed through the prism of cost-benefit analysis, perhaps the cost to privacy and related human rights associated with the upholding of this narrative far outstrips the security gains now and in the future.

Conclusion

Undoubtedly the post 9/11 anti-terrorism policy resulted in entrenching mass surveillance regimes particularly in Europe, with repeated scepticism as to its tangible benefits in terms of achieving national security. In this sense alone, the legacy of 9/11 will likely resonate for years to come and facilitate further expansion of state surveillance powers not only in consolidated but also in backsliding democracies. In Hungary and Poland, for example, the authorities have significantly expanded their surveillance powers without meaningful oversight mechanisms in place, whilst Polish security services have allegedly been using Pegasus malware to spy on the ruling party's opposition politicians. The

ECtHR legitimising bulk interception practices coupled with the legislative branch often too willing to grant the executive blanket and unconditional powers of mass surveillance in the name of fighting international terrorism seem a flimsy bulwark against surveillance industry. Yet, this is the unquestionable and unfortunate result of the global culture of counterterrorism narrative which has been successfully propelled by the politics of fear since 9/11.

Gefördert durch die bpb: Bundeszentrale für politische Bildung

---

SUGGESTED CITATION Watt, Eliza: *The legacy of the privacy versus security narrative in the ECtHR's jurisprudence, VerfBlog,* 2022/4/21, https://verfassungsblog.de/os6-privacy-vs-security/, DOI: 10.17176/20220421-182404-0.

Explore posts related to this:

LICENSED UNDER CC BY SA