Function creep, altered affordances, and safeguard rollbacks

Markus Naarttijärvi 2022-04-11T11:13:45

”*According to this committee, it is thus hardly thinkable to provide possibilities for surveillance measures on such comparatively vague justifications as the terrorism act provides in order to provide protection against serious crimes in general. This would presume pervasive changes of the rules of criminal procedure that from a principled point of view would appear extremely dubious. There is in fact no doubt that the surveillance measures provided by the terrorism legislation deviates from the requirements of legal certainty that has traditionally been maintained in this country.*”[1)]All translations are the author’s own.

– Committee on terrorism legislation, 1989 (SOU 1989:104 p. 219)

“*The fact that information can be obtained relatively broadly and unconditionally is necessary for the intelligence work to be conducted efficiently. Excessive regulation risks hindering collection in an undesirable way.*”

– Swedish Government bill on law enforcement access to communications metadata (Prop. 2011/12:55 p. 84)

Leaving a paradigm behind

Stating that the terrorist attacks on 9/11 led to a paradigm shift in the political and legal approaches to surveillance of the private sphere is an observation so obvious it may sound like a platitude. Still, it remains valid. But where it used to be a statement about the events shaping our current paradigm, it may now soon become an observation about the past. We still don’t know how the illegal, unjustified, and senseless war of aggression Vladimir Putin currently wages in Ukraine will impact the legal frameworks surrounding surveillance and privacy. But looking back at the 20 years of legal development since 9/11, is perhaps even more pertinent now, as it allows us to see not only that a shift occurred, but also more clearly how that shift was manifested. This in turn can teach us about what we may expect going forward.

In 2013, I published my PhD thesis on the rise of preventive electronic surveillance measures in Sweden. In it, I traced the development from the early days of telephone surveillance in the post-war era to the modern preventive electronic network surveillance and signals intelligence, focusing on the mandates provided to the Swedish Security Service (*Säkerhetspolisen*). Using constitutional proportionality theory as a lens, I sifted through preparatory works published between 1945 and 2013 to analyze the balancing of security and privacy interests within the legislative processes leading up to expanding surveillance mandates.

Having gone through that process, I concluded my thesis on some rather gloomy observations. I found that legislators had largely failed to acknowledge the increasingly intrusive nature of surveillance that technological developments had brought. Statements on the privacy implications of certain measures were simply reused over the years with little consideration of fundamentally altered technological affordances shaping those implications. As we know, the use of metadata surveillance to register numbers called from landline in the 1960's is fundamentally different from the minute-to-minute geolocation and surveillance of mobile communication devices today. We also know that communications metadata can now be analyzed on a larger scale, more quickly, and provide insights that even communications content may not. Yet, the same analysis of the privacy implications of metadata surveillance – holding it as significantly less sensitive than communications content surveillance – was essentially reused repeatedly and almost verbatim by legislators throughout the years.[2)] This continued until the CJEU acknowledged the implications of meta data surveillance in the *Digital Rights Ireland* and *Tele2* judgements, essentially equating the privacy implications to that of content surveillance and thereby forcing the legislator to change approach.

Another conclusion was that each reform towards preventive surveillance outside of the context of criminal procedure was presented as non-exceptional, once that first step had been taken. Each successive step from the paradigm of reasonable suspicion towards an increased role of risk-based logic would look back on a previous example that proved that this new proposal was neither unprecedented nor exceptional. Looking a bit closer at those legislative precedents, however, reveals even more clearly the fundamental shift that happened during the years following 9/11.

A temporary firewall

The first real, albeit limited step towards preventive surveillance mandates in Sweden was taken in the early 1970's through the 'Terrorist Act'.[3)] The official name was Lag (1973:162) om särskilda åtgärder till förebyggande av vissa våldsdåd med internationell bakgrund ('Act (1973:162) on special measures to prevent certain violent acts with an international background'). This Act provided a narrow set of measures for when the deportation of a person believed to be a member of a terrorist organization could not be carried out on account of non-refoulement concerns.[4)] The organization the individual was engaged in would also, through their previous activities, have to have shown that they systematically used foreign land as a scene for violent actions with political purposes. The targeted individuals (usually numbering no more than 0-3 persons in a given year) could then be made subject to certain preventive surveillance measures, including the tapping of phones following a court order. The measures were intended to ensure that these individuals, or an organization they belonged to or acted for, did not engage in terrorist activities while remaining in Sweden. In establishing this measure, the legislator made it clear that it constituted a significant departure from established privacy norms and legal safeguards, and that the legislation could be accepted only as it pertained to a very

limited cadre of individuals, already subject to eventual deportation on national security grounds.

For some time, this firewall of principle separating the wider public from similar measures held fast. In the wake of the murder of prime minister Olof Palme in 1986, a parliamentary committee considered widening the Terrorist Act to Swedish citizens and foreigners not yet subject to deportation orders, but ultimately found that 'the evidentiary requirements in the regulations are so low that it can hardly be considered justifiable to provide for the possibility of coercive measures in the event of even weaker suspicions.' (SOU 1988:18, p. 170–171). They also concluded that the exception for foreigners subject to deportation orders could ‚be considered justifiable only as an outgrowth of our right to decide for ourselves which foreigners are allowed to stay in this country. To make further exceptions is out of the question.' (Ibid. p. 175). The following year another inquiry tasked with evaluating the need for wider preventive surveillance measures found that such a proposal would unacceptably undermine established rule of law principles. These findings were reached despite the committees being mindful of 'the ever-increasing or at least uninterrupted high frequency of terrorist acts and their geographical spread' (SOU 1989:104, p. 179).

The new reality

With the terrorist attacks on 9/11 and in London and Madrid in the following years, this firewall began to crumble. In accordance with the trend in most western states, what was once regarded as unacceptable from a rule of law standpoint slowly became implemented as part of the new security paradigm. Through the '2007 Prevention Act'[5)]The official name is Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott ('Act 2007:979 on measures to prevent certain particularly serious crimes'). the Swedish Security Service was given a wider mandate to use preventive electronic surveillance to counter terrorism and certain other crimes against national security. In justifying this measure, the government leaned against the existing rules in the Act on measures against foreigners subject to deportation, arguing that the new measures were not, in fact, unprecedented or a significant departure from existing norms. A line of argument that required some very skillful cherry-picking from the historical context and previous legislative deliberations. In fact, the new rules must be seen as a legal watershed moment towards a normalization of the preventive security paradigm and caused a fundamental shift in how covert surveillance could and would be deployed.

The next significant step was taken in 2012, when measures for preventive metadata surveillance was introduced. The new law, colloquially called 'the Gathering Act',[6)]The official name is Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ('Act (2012:278) on the gathering of information about electronic communication in law enforcement authorities intelligence operations'). gave law enforcement agencies access to historical (as opposed to real-time) communications metadata, including the past location of specific communication

devices. This Act is significant in two regards. First, the government – as apparent from the quote in the beginning of this essay – specifically intended a broader and more unconditional gathering of communications data. This led to the adoption of conditions for access to information based not on specific levels of suspicion, but rather the benefit the information could bring for law enforcement agencies, i.e., whether it could be of 'particular importance' in preventing, deterring, or detecting crimes that could warrant a prison sentence of two years or more. Second, the legislator did not find it suitable to place the authorization for these surveillance warrants on any external authority like a court, but rather internally within law enforcement agencies themselves. The rationale for this was based mainly on practical and organizational concerns relating to expedience, but the government added the more principled argument that unlike in the crime investigation context, the privacy dimension in intelligence operations was not characterized by an adversarial dimension but rather displayed more of a 'citizen perspective', which was not as well suited for courts to decide on (Government bill. 2011/12:55, p. 88–89). There is so much one could say on that point, but I'll settle on observing that perhaps the government felt that law enforcement agencies with a vested interest in access to data would, in fact, be better suited to take that citizen perspective into account than a court of law. More likely however is that a court might get in the way of that 'more unconditional' gathering of communications data the government had in mind. In 2019, the power to authorize gathering of meta-data was moved to prosecutors who are organizationally separate from the police authorities. This was a result of the Tele2 judgment (Joined Cases C#203/15 and C#698/15), requiring authorization by a court or independent authority. It is uncertain if this move fulfills the requirement of an independent authority, but it must be seen as a step in the right direction.

These reforms may well be described as examples of surveillance or function creep, in that they represent a stepwise and creeping expansion of surveillance mandates. Further expansions of preventive surveillance measures to counter organized crime are currently being considered, so the development has by no means stopped.

Safeguard rollbacks

It is however also worth highlighting a parallel development of equal importance, through what could be described as *safeguard rollbacks*. These are different from surveillance creep, in that the aim and purpose of surveillance mandates remains largely the same, but the associated safeguards are gradually weakened. These rollbacks have generally taken place where mandates were initially put in place with strict limits to ensure proportionality and legal certainty, but where the effectiveness of those mandates are later argued to be limited due to the safeguards themselves.

A telling example is how the government changed the legal definition of which individuals could be subject to preventive surveillance by the Swedish Security Service in the previously mentioned 2007 Preventive Act. When the act was initially proposed, the legislator took care to differentiate it from the rules established in the 1970's Terrorist Act. A more significant individualized assessment was highlighted as a safeguard, where association with a specific organization would not be a determining factor, only whether there was 'particular reasons to assume' that a

specific individual would commit a specific range of serious crimes, such as terrorist crimes. This essentially created an evidentiary standard for interferences where credible information needed to point towards future specified crimes. A subsequent evaluation found, however, that this requirement became difficult to reach in practice. Actual evidence of future possibilities was both difficult to come by and would end up leading to the opening of a formal investigation into preparatory offences. This analysis eventually led to a revised threshold implemented in 2015. This was based on whether there was a 'significant risk that a specific person would engage in' certain serious criminal activities. The organizational connection now made a comeback, as this 'significant risk' threshold in relation to a specific individual would be lowered in cases where there was a significant risk that an organization the individual 'belonged to or acted in support of' would engage in the serious criminal activities. In such cases, the threshold would be reduced in relation to the individual, where it would suffice that the individual 'may be likely (*befaras*)' to support these activities.

Another example can be found in the legal rules surrounding the collection of signals intelligence in electronic communication networks. When in 2008 the Swedish defense radio establishment (FRA) was given the mandate to collect signals intelligence in fiber optic cables carrying electronic communication to and from Sweden, the fierce public and political backlash surrounding the reform forced the government to draw clear boundaries between law enforcement and military intelligence gathering. It was said that the signals intelligence conducted to further defense interests was aimed at foreign threats to national security and would not be allowed to undermine the rules governing the use of electronic surveillance under the rules of criminal procedure. As such, both the Swedish security service and the national police were initially excluded from directing the intelligence gathering but could still receive intelligence reports relevant to their tasks from the defense radio establishment. In 2013 however, the Swedish Security Service and the National Operations Department of the police were given the mandate to direct signals intelligence gathering towards phenomena they had an interest in. To compensate for this new mandate, police agencies were not allowed to receive intelligence about matters relating to ongoing criminal investigations. Eventually, the government found that this was unpractical. It could lead to a situation where if information emerged that indicates that an international terrorist organization was planning a terrorist attack in Sweden, and the suspicions would reach such a level a preliminary investigation was opened, the FRA would need to suspend its reporting to the authority. Hence, in 2019, this limit was also removed. Instead, a rule was issued stating that the national police and the security service could not use the information they received within criminal investigations and information from signals intelligence should (as a main rule) not be given to persons involved in such investigations.

What have we learned?

In light of the Swedish example, we can see developments of government electronic surveillance occurring along at least three developmental axes. First, there is the increased depth of surveillance measures in terms of the resolution of the picture that they draw of the individual, driven to a significant degree by changes in the

underlying technologies of communication and data processing. On the second axis is the expansion in terms of width or scope, i.e., the range of individuals, groups, or phenomena potentially subject to surveillance. This is where most discussions of surveillance or function creep will tend to focus, and we can indeed see that the concept is alive and well in Sweden in relation to preventive surveillance. Finally, on the third axis, we find the safeguards implemented to prevent abuse of the measures implemented along the first and second axis. Here, the Swedish example suggests that we need to pay closer attention to safeguard rollbacks. The sometimes intricate and legal-technical nature of these rollbacks are less likely to attract political and public interest, yet they may carry far-reaching implications in the practical effects of surveillance mandates. Proportionality reviews by European Courts have so far proven to be the main limit to government ambitions in this regard, as they tend to place great emphasis on existing safeguards rather than placing outright limits on surveillance as such. Finally, along all these axes we need to pay close attention to changes in the technological affordances which may alter the practical effects of legal mandates or allow the introduction of methods to arise within or in between existing mandates. As the mandates and legal safeguards surrounding surveillance begin to face the capabilities provided by technologies of machine-learning and automated decision-making, this is likely to become more important than ever.

References

- All translations are the author's own.
- This continued until the CJEU acknowledged the implications of meta data surveillance in the Digital Rights Ireland and Tele2 judgements, essentially equating the privacy implications to that of content surveillance and thereby forcing the legislator to change approach.
- The official name was Lag (1973:162) om särskilda åtgärder till förebyggande av vissa våldsdåd med internationell bakgrund ('Act (1973:162) on special measures to prevent certain violent acts with an international background').
- The organization the individual was engaged in would also, through their previous activities, have to have shown that they systematically used foreign land as a scene for violent actions with political purposes.
- The official name is Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott ('Act 2007:979 on measures to prevent certain particularly serious crimes').
- The official name is Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ('Act (2012:278) on the gathering of information about electronic communication in law enforcement authorities intelligence operations').