Origins, transnational trajectories, and current dilemmas

VB verfassungsblog.de/pnr-security/



Didier Bigo



Stefan Salomon

This article belongs to the debate » The Future of the European Security Architecture: A Debate Series
09 Mai 2023

Passengers Name Records and Security

Security is not a transparent concept, but a contested one. There is no single form of security (national or global), but different forms of security (or in-security processes) that might be contradictory and mutually destructive. That is true for the notions of “preventive security” on the one hand, and of “policing security” on the other. The latter refers to targeted actions which respond to prognoses about concrete individual cases. Its legal framework is that of criminal law, based on a logic of inquiry, evidence-based investigation, and the presumption of innocence, even when it involves intelligence-led policing. In contrast, the new paradigm of preventive security relies on generalised surveillance and on a logic of general suspicion. Its principal legal field is that of administrative law and it operates through predictive tools that produce new ‘realities’ by establishing correlations and patterns between seemingly unrelated facts. In this sense, preventive security is creative – not merely reactive. Preventive security and policing security are largely incompatible.

The EU Passenger Name Records (PNR) Directive is based on the logic of preventive security. In this post, we describe the emergence of preventive security, how it entered into and eventually transformed PNR collection from a commercial activity into a security tool, and radically reshaped the work of border guards. Finally, we highlight the possible effects of the Court of Justice of the European Union (CJEU)’s PNR decision (*Ligue des droits humains*) on the operation of preventive security measures. We argue that the judge of the CJEU did not simply accept a preventive security argument, and curbed its expansion, which may help security services to enhance their efficiency and legitimacy.

Inventing “preventive” security via “predictive tools”

Following the events of 9/11 in the US, the 9/11 Commission Report and the administration under President George W. Bush considered that policing as security practice had become obsolete in light of the peculiar threats that the US faced. The terminology of 'terrorist attacks', adopted by the US administration, shifted the terrorist acts by Al-Qaeda and Osama bin Laden from grave criminal acts into the register of war. This, in turn, triggers particular executive privileges, limited judicial review and an elevated role for intelligence services fighting an allegedly "stealth" enemy. The covertness of the adversary and the US government's fear of a possible use of biological, chemical and nuclear weapons resulted in policies that sought to anticipate terrorist acts *before* they happened. Donald Rumsfeld, then Secretary of Defence in the Bush administration, famously claimed that it was necessary to discover and anticipate unknown unknown threats through Total Information Awareness (TIA). TIA, renamed later to Terrorism Information Awareness, was a mass surveillance program under the portfolio of the Department of Defence.

The objective of the TIA program was to collect and systematically correlate all electronic data on passengers landing on US territory through integrating different information technologies. The use of technologies capable of detecting 'weak signals' – the hidden network of relationships a data point has within vast amounts of data on the past and present behaviour of passengers – was seen as a revolutionary method to prevent terrorist offences. It was legitimised by the 1% doctrine: if it was necessary to surveil and detain 99 innocent persons in order to identify one terrorist, the measures were considered justified.

In September 2003, the US Congress eventually defunded the TIA program due to concerns about the mass collection of US citizens' personal data. However, US intelligence services continued to use several of the TIA program's features. The US government considered internet and smartphone surveillance, along with tools to locate and identify passengers travelling to US territory, as the way forward to ensure national and global security in a context of transnational terrorism.

The origins, expansion and complexification of PNR

The use of PNR data as a security tool was a result of the idea that it was necessary to "act before the next attack". Congress adopted the US Aviation and Transportation Security Act in order to monitor passengers and generalise electronic pre-border checks, despite concerns of airline carriers, foreign governments and the International Airline Transport Authority. Airlines which refused to transfer their commercial passenger data to US authorities would not be permitted to operate on US territory. In order to transfer passenger data, airlines were required to organise their information based on a PNR list of 34 security criteria (further reduced to 17 in 2016), which included relational and situational elements, such as the seat number, used to check whether nearby seats were occupied by a suspected person. The US Aviation and Transportation Security Act therefore transformed PNR data from a mere commercial activity by airline carriers into a security tool for US authorities.

The origins of PNR data use as a security tool are clear. However, global reactions differed. While some countries were averse to the idea that their national airline carriers would transfer PNR data to US authorities, others were enthusiastic. The EU, among others, concluded an agreement with the US on the transfer of advance passenger information and PNR data. The UN Security Council, in the context of foreign nationals travelling to Syria to join the Islamic State, elevated the transfer of PNR data to a global "best practice" standard that all UN member states should adopt in their national laws (UNSC Resolution 2178 (2014), para 9-11 and UNSC Resolution 2396 (2017)).

At the same time, concerns emerged about the protection of personal data, among others. In 2017, the CJEU held in Opinion 1/15 that the EU-Canada PNR agreement would be contrary to Articles 7 (respect for private and family life), 8 (right to protection of personal data), and 21 (right to non discrimination) of the Charter of Fundamental Rights of the European Union, among others, because the agreement neither prevented the transfer of sensitive personal data to Canada, nor discriminatory results of data processing. In a similar vein, the Council of Europe's Consultative Committee of Convention 108 highlighted that PNR measures strongly interfered with the right to data protection under the European Convention of Human Rights. Although human rights, especially the right to protection of personal data, became a gateway to criticise the preventive security paradigm that undergirds PNR measures, the human rights critique did not directly address the principal issue concerning PNR data: the *shift* to generalised preventive security.

Moreover, the complexification of PNR from its origins to the present day is a process in which multiple interests have reshaped the regulatory landscape. In this process, the EU has not simply followed US developments. The PNR Directive is born also from the EU's preoccupations with irregular migration. Already in the 1990s, years before the adoption of the PNR Directive, European police authorities integrated information on crime, terrorism, and irregular migration through the Schengen Information System (SIS), thus maintaining access to different datasets for police and border guard authorities. The 2004 Madrid bombings then contributed to a considerable function creep. Police authorities increasingly gained access to databases used for other purposes than crime, especially databases on asylum and border crossings – a trend which was further reinforced by SIS 2 in 2013, which upgraded the SIS into a search engine.

The process of rendering databases interoperable was mainly driven by data engineers and intelligence services. Although anti-terrorist specialists at police authorities considered that internal threats would not be addressed by shifting the policy focus on external threats, they nevertheless considered it useful to add border control as an additional layer to already existing surveillance instruments. The narrative that democratic governments are active and closely cooperate to protect their population based on a strategy of prevention and prediction (the famous 3Ps), provided public legitimacy to expanding instruments of intelligence services to areas of policing and immigration

control. The upshot is that the legitimacy of the idea of preventive security remained unchecked, appearing as additional – and not contradictory – to the logic of security in policing.

Transformations of security professionals' practices

The expansion of surveillance instruments and the consolidation of preventive security in immigration controls over the last twenty years fundamentally changed the everyday work of border guards. Border guards, who are at the frontline of controlling travel documents, turned into a sort of secondary policemen. This created unease about the 'intelligencification' of their activities and uncertainties among border guards on what their role actually is.

At the same time, the development of human and technological resources, which organise the interoperability of databases for collecting, storing, sorting, and sharing passengers' data, remained largely shielded from public attention. These developments involved not only public but also private actors with considerably greater resources to produce more accurate technology within a shorter span of time. Technological developments in the private sector occurred especially through the advance of proprietary software, often shrouded in secrecy, that use algorithms and machine-learning processes. Algorithms and machine learning, in turn, facilitate the use of predictive tools that establish risk scores and assign personalised risk factors to suspects on watch lists.

The result of these developments was the normalisation of surveillance technologies developed by the private sector beyond their commercial use. These technologies' margins of error remain significant: more than four out of five individuals flagged by PNR measures are false positives, and thus subjected to false suspicion (see this report from the oral hearing preceding in *Ligue des droits humains*). From the perspective of security studies, the expansion of mass surveillance technologies in the context of the 'war on terror' fundamentally changed the idea of the presumption of innocence (see here for an example).

The CJEU's PNR decision: recalibrating preventive security measures?

We focus here only on three points in *Ligue des droits humains* that relate to the preventive security dimension and different interpretations of what "preventive" may mean.

First, the application of the PNR Directive, where the Court distinguished between the internal and external dimension (intra-EU flights versus flights from third countries to the EU). In regard to the latter, the Court argued that the "very nature" of the threats would justify the systematic collection and transfer of PNR data to member states (see para 162). Excluding certain areas or groups of passengers would hamper the objective of the PNR Directive, namely, to identify persons who may present a risk to public security "from among all air passengers" (para 161). However, when it comes to intra-EU flights, the

CJEU makes clear that a member state may only apply the PNR Directive if there are solid reasons to assume that it faces a genuine and present threat of serious crimes or terrorist offences. Moreover, the application of the PNR Directive to intra-EU flights must be strictly limited to the duration of the threat and to specific flight routes or airports (paras 171-172). The Court essentially uses a spatially stratified strict necessity test, which reflects two different meanings of “preventive security”. Internally, the Court requires a reasonable suspicion for the existence of a particular threat. The Court thus bends member states’ global preventive security logic towards a more targeted and reasoned logic of classical intelligence-led policing based on evidence in the EU . In other words, the application of the PNR Directive for intra-EU flights is conceptually viewed in the framework of policing security and not in terms of preventive security. Externally, the preventive security paradigm and general suspicion continue to reign.

Second, the CJEU considered, as it had already done in Opinion 1/15, that the collection of PNR data seriously interferes with the right to the protection of personal data under the EU Charter on Fundamental Rights. Any processing of PNR data must therefore be “strictly necessary” and limited to the purposes of the PNR Directive, that is, combating ‘terrorist offences’ and ‘serious crime’ (paras 148 et seqq.). In this regard, the CJEU was particularly concerned about security and intelligence agencies using PNR data as mere search criteria for data mining in various other databases, and for other purposes than the PNR Directive intends. Therefore, the Court limited database interoperability: it made clear that the Passenger Information Units (PIUs) may compare PNR data only to databases on persons or objects sought or under alert (paras 182 et seqq.). Security and intelligence services are thus not permitted to process PNR data only because it gives them the possibility to nurture the predictive capacity of their databases.

Third, the willingness to predict through algorithms is based on the belief that the detection of anomalies or weak signals, which emanate from a small statistical group that shares the same characteristics, is only valid if the number of data initially collected is “large”. The systematic collection and storage of data over a long period of time is crucial for the functioning of any algorithm. This implies automatic processing of large amounts of data in which human intervention is limited to monitoring the process and intervening after sorting in a very limited number of cases. The Court, however, insists that human intervention must remain capable of understanding the specific reasons why an algorithm arrived at a positive match (para 210). The Court thus reintroduces a logic in which correlations are not enough to establish suspicion. Rather, causality is needed to establish ‘reasonable’ suspicion – and not a ranking in which many people may have high scores for bad reasons.

Conclusion

Instead of accepting a preventive security argument, the judges of the CJEU brought some reason into a derailed logic of collecting ever more data. In addition to curbing the expansion of preventive security, the PNR judgement may also help security services to enhance their efficiency and legitimacy. Security services do not seem to believe in Chris

Anderson's slogan that "data thinks for itself" and that we have reached "the end of theory because the flood of data is now making the scientific method obsolete". Rather, the work of security services is based on hypotheses, theories, research and evidence; in other words, on conjectural reasoning, as Carlo Ginzburg argues in his analysis of truth, history and security.

Contrary to studies that highlight the growing role of technologies in the design of an algorithmic security apparatus organised around quantitative techniques of knowledge production, Laurent Bonelli and Francesco Ragazzi show that the heart of counter-terrorist intelligence gathering is largely a matter of using qualitative and analogical techniques: informants, interpersonal relationships and the operationalisation of knowledge through traditional methods such as writing reports, notes and summaries.

Ligue des droits humains thus offers an opportunity for national judges to question more radically the idea of generalised preventive security that seeks to anticipate human behaviour through the creation of risk profiles and statistical correlations (instead of causality). Judges should question more directly the idea of preventive security and seek clarifications on what constitutes 'reasonable suspicion'. For without proper justifications, 'reasonable suspicion' is kind of an oxymoron.

LICENSED UNDER CC BY SA
SUGGESTED CITATION Bigo, Didier; Salomon, Stefan: *Passengers Name Records and Security: Origins, transnational trajectories, and current dilemmas, VerfBlog,* 2023/5/09, https://verfassungsblog.de/pnr-security/, DOI: 10.17176/20230509-163317-0.

Explore posts related to this:

Other posts about this region:
Europa
LICENSED UNDER CC BY SA