Simon Egbert

40 Platforms

Abstract: This chapter focuses on one of the latest technical developments (not only) in police work: the emergence of data integration and analysis platforms. The police use these platforms to seamlessly combine data from different sources and to make it easier to analyze. These platforms are updating the myth that lots of data promises relevant findings and are also reproducing an association-centered logic of knowledge production. This is closely linked to the risk of increased surveillance.

Keywords: data integration and analysis platforms, Palantir, police, network, surveillance, algorithms

This chapter focuses on a technical tool that plays an increasingly important role in digital societies: data integration and analysis platforms. Most, if not all, criminological relevant organizations in digitized societies will (have to) work with such or similar tools in the future. Because these platforms will be used to cope with the constantly increasing mass of data and to maintain analysis capability. Therefore, this chapter provides an overview of the current proliferation of data integration and analysis platforms with special emphasis on platforms from the US software company Palantir and their utilization in the field of policing.

While the phenomena related to the term ‘digital platform’ are very diverse, they still share some basic traits: a connectivity-oriented infrastructure that aims to facilitate interactions by at least two third parties and a mode of functioning based on massive and diverse data, as well as a modular architecture (e. g., Andersson Schwarz, 2017; van Dijck et al., 2018). With this definition in mind, data integration and analysis platforms are understood here as digital platforms that aim at making available heterogenous data from different sources, especially by facilitating cross-connections and desilozation to generate relevant and actionable associations.

While focusing on platformized policing in this chapter with regard to data integration and analysis platforms, it needs to be highlighted that already other understandings on platformized policing exist (see Policing by Wilson). For example, Wil-

Disclaimers and Acknowledgments: This chapter has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (Grant agreement No. 833749). I acknowledge support for the publication costs by the Open Access Publication Fund of Bielefeld University and the Deutsche Forschungsgemeinschaft (DFG).

son's (2019, 2021) work on the increasing use of cloud services by police forces or Gates' (2019) analysis on the role of Axon as a police platform, trying to generate revenue with (police) data, ultimately seeking to redesign the police organization as a platform in its entirety (see also Wood, 2019). It must also be emphasized that not only the police, but also other criminologically relevant organizations, especially intelligence services (see Intelligence by Gundhus and Lundgaard), use these technologies (Biddle, 2017). And not only that, but such platforms are also already being used in other, quite different areas of society, for example by the United Nations World Food Programme (Matak, 2021) or the National Health Service (NHS) in the United Kingdom (Mason, 2023). Although the US-software company Palantir, which can be considered the current market leader of data integration and analysis platforms for policing with its platform named 'Gotham,' is the main reference throughout the text, other comparable solutions do exist, like the open-source 'KNIME' Analytics Platform (KNIME, 2024), Hitachi Vantara's 'Pentaho' Data Integration and Analytics platform (Hitachi Vantara, 2024), Atos' 'research and analysis platform' (Atos, 2022), or 'rsShadow' by Rola security solutions (Rola Security Solutions, 2024).

The argumentation of this chapter is structured as follows: first, we will present a short overview of the use of platforms in police agencies of different countries around the world, which leads us to the thesis that police are becoming increasingly platformized. Second, we will focus on the key functionalities of data integration and analysis platforms. After that, we will discuss the societal risks of police forces using these platforms. In the conclusion, we summarize our argument and provide pointers for future digital-criminological research.

The platformization of policing: an empirical overview

As is so often the case when it comes to new technological developments in policing, US police forces are the pioneers of platformization. The first known Police Departments using Palantir Software come from the Salt Lake Valley, in which Palantir software was used *inter alia* by the Salt Lake City Police Department since 2010 (Palantir, 2012). Especially referring to the Palantir Graph application, the police force focused on investigating criminal networks, using data from different sources: mug shots, airport data, criminal records, suspicious activity reports, among others (Hardy, 2016; Palantir, 2012). Also, the Los Angeles Police Department (LAPD) was early adopting Palantir's Gotham platform (Brayne, 2021; Ferguson, 2017). The LAPD used it from 2011 onwards, when it played a major role in the Los Angeles' Strategic Extraction and Restoration Program, also known as Operation LASER, which aimed at reducing gun-related violence by focusing on gang members and repeat violent offenders (Ferguson, 2017: 102 – 103; Uchida et al., 2012). The platform was used to create so called 'Chronic Offender Bulletins,' overviews of the criminal careers of relevant offenders, plus to produce information on their spatial and personal environment, accessing police data like information from license plate readers or field information cards (Brayne, 2017: 986–987). In 2012, Palantir software was implemented by the local police in New Orleans, as part of the 'NOLA for Life' initiative launched by Mayor Mitchell J. Landrieu, which aimed at implementing a "comprehensive murder reduction strategy" (City of New Orleans, 2013). Palantir's Gotham software was used in this for building a unified data environment consisting of internal police data banks and public data sources, most notably police and public safety data as well as information on infrastructure, like the location of liquor stores, hospitals, or parks (Ferguson, 2017: 41).

In other countries, data integration and analysis platforms are implemented and used by police forces as well. In Norway, for example, Palantir's Gotham platform was purchased in 2016 to connect data from 19 different police databanks in a project with the characteristically name 'Omnia' (meaning 'everything')—which has cost close to 100 million Norwegian kroner (approx. US$14 million) but has ultimately failed (Gundhus and Wathne, 2024). Palantir Gotham is also used by the Danish police, where the system is called POL-INTEL, becoming fully operational in 2018 (Galis and Karlsson, 2024). In Germany, three federal police forces use modified versions of Palantir's Gotham (Ulbricht and Egbert, 2024). Palantir software has also been used at the supranational police level, namely by Europol from 2016 to 2021 (European Parliament, 2020).

Key characteristics of data integration and analysis platforms

What specifically makes data integration and analysis software so attractive for police forces and what technical characteristics are associated with this?

The primary goal of these platforms is to make analysis and research processes faster by connecting heterogenous data from different sources and by making them accessible from one central digital location. Being a special type of digital platform (see Ulbrich and Egbert, 2024), data integration and analysis platforms share important similarities with the well-known internet-based digital platforms such as Amazon, Facebook, or Uber (van Dijck et al., 2018). However, they also have important differences: instead of connecting third parties and receiving fees for this service, as in the case of for example Uber or Airbnb, data integration and analysis platforms connect their clients with data, as well as data (banks) among each other. By doing so, they try to enhance interoperability, the "so-called smart way to connect the dots and to avoid continuing to work in 'silos' with segmented information networks" (Bigo, 2020: 410), which is reflected in Palantir's main goal of the 'desilozation' of information systems (Palantir, n.d.: 2).

Of course, desilozation is not a value in itself, but follows a specific rationality: by being able to look at different data sources at the same time and to relate the data they contain with each other, new knowledge shall be produced. In the field of police, this idea has been known for years and has already emerged along with the first algorithmic analysis procedures (see e. g., McCue and Parker, 2003) and is updated by Palantir by offering their platforms “as the connective tissue between an organization’s data, its analytics capabilities, and operational execution” (Palantir, 2020).

An illustrative example of the knowledge creation potential connected to data integration and analysis platforms is the already mentioned graph application from Palantir’s Gotham platform. It provides a space for performing link analysis and is one of the most critical applications for communicating (provisional) analytical conclusions. The graph application implements the link analysis and association-centered analytical approach of Palantir Gotham in a very direct way, it can be thus characterized as its analytical core. Via a spider diagram architecture, it allows to show associations between people or objects in a visually convenient and actionable way, allowing to identify relevant connections by police analysts at first glance (Brayne, 2021).

However, data integration and analysis platforms are not only about producing new knowledge, but also about speeding up decision-making processes and rendering police work more efficient. Providing a unified data environment, data integration and analysis platforms make heterogenous and numerous data sources available with one click, instead of enabling access only individually, with recourse to separate programs and formal access procedures (Iliadis and Acker, 2022).

And even if there are many points of criticism associated with these platforms (see below), the criticism of automation that is otherwise often expressed with regard to algorithmic decision-making systems is only partly applicable here (e. g., Algorithm Watch, 2020). This is the case because data integration and analysis platforms imply a special socio-technical interaction, meaning that algorithms and analysts *together* generate new knowledge and, hence, inform decisions. And although the platforms themselves play an important role in these processes, similar to their better-known platform siblings from the internet (like YouTube and Facebook), data integration and analysis platforms are commonly framed as neutral intermediaries (e. g., Gillespie, 2010). In the words of Palantir: “We build digital infrastructure for data-driven operations and decision-making. […] We license this software to organisations, who receive secure and unique instances of our platforms in which to conduct their own work on their own data” (Palantir, 2020). As opposed to dismissing the platforms’ generative and transformative role, we should, however, understand these platforms as mediators, as van Dijck (2013: 29) suggests.

Risks

A risk which is connected to policing in general, but to platformized policing in specific, refers to surveillance (see Surveillance by Lyon). As described, the goal of data integration and analysis platforms is the connection of diverse data sources to make existing data more easily analyzable by police officers. Surveillance is the immediate flip side of this approach, because the operational idea of data integration and analysis platforms is built on the well-known big data-myth that one only needs enough data to discover new, hitherto unknown connections (e. g., Anderson, 2008). This approach implies that every attempt should be made to utilize and integrate as much data as possible into the platforms. This can ultimately serve as incentive to interpret legal access restrictions to data as narrow as possible, and, if necessary, also to exceed these limits (Egbert, 2019). This is one of the reasons why Iliadis and Acker (2022) name Palantir's software a 'surveillance platform.'

One practical implication of the close relationship of these platforms and surveillance is what Brayne (2021: 112) calls "net widening," meaning that the number of persons who come into the police's focus will increase, since police analysts will increasingly use platforms to check persons who have not yet been processed by the police and who have so far only been indirectly involved with the police, for example witnesses or associates of serial offenders (friends, family, etc.). This is based on an approach which Brayne (2021: 39) terms "dragnet surveillance," that is the "collection and analysis of information on everyone, rather than only people under suspicion," which implies lowering the threshold above which citizens are subject to police control. Although Brayne refers this approach to digital policing in general, it applies to data integration and analysis platforms in specific, because they provoke the reversion of an important principle of police work with regard to civil rights: Instead of checking a person more closely when a suspicion against them arises in the course of the investigation, people are now monitored in order to establish such a suspicion in the first place.

A special problem associated with data integration platforms given the low barrier to entry into police data systems can be called 'risk/suspicion by association.' This principle means that an individual is perceived as suspicious or risky because—according to the data available to the platform—it interacts with (past) offenders and/or known high-risk persons. Since information about the social milieu and entourage play an important role in the social network- or "associational suspicion"-approach facilitated by data integration and analysis platforms, their utilization not only indirectly harbors the risk to materialize this principle (Ferguson, 2017: 200).

According to Brayne (2021: 116), dragnet surveillance also includes that those people who were already in the police's focus before, are now being monitored even more closely, since their data are analyzed across increasing and diverse institutions (besides police, also social services, or banks, for example). This in turn can lead to a 'vortex' of disadvantage, because people who are more intensely controlled by the police have increasingly worse chances of, for example, getting a loan (Brayne, 2021; Eubanks, 2017). And this dynamic is also a problem precisely because police data tends to be systematically biased, since police officers in many countries of the world tend to be racially biased in their control and reporting behaviour, which then inevitably affects the quality of the police database and the decisions that are made based on this data (e. g., Richardson et al., 2019). In fact, the LASER project of LAPD was criticized precisely because of the 'vicious circle' it creates with the help of Palantir platforms by integrating low-threshold data (e. g., field interview cards) that are collected based on the (biased) spatial and person-related selection decisions made by police officers (Bhuiyan, 2021). The use of platforms, then, ultimately leads to precisely these areas and people coming under even more police scrutiny, since platforms necessarily identify those areas or people as more suspicious that are overrepresented in the data sets accessible to them.

The socio-technical constellation connected to data integration and analysis platforms mentioned above entails that it is particularly difficult to reconstruct its knowledge creation and decision-making processes retrospectively, which is, ultimately, detrimental to the transparency of police work. However, although the human part in this process is important, we should not make the mistake of devaluing the platforms' share of the analytical work. Even the compilation and processing of data represents an analytical intervention that should not be underestimated in its epistemic relevance (Galis and Karlsson, 2024). Data integration and analysis platforms specify which data can be considered by human analysts and, hence, with what probability they are processed. In addition, the very representation of connections is already charged with suspicions and risk attributions, with at least subliminally reproducing a logic of 'risk/suspicion by association.'

A final risk that is associated with data integration platforms is connected to the question of what happens to those data or results that have been viewed and generated with the help of the platform. A dispute between the New York Police Department (NYPD) and Palantir in 2017 shows that it can lead to serious problems when such collaborations end. In this specific case, the NYPD decided to use a new software and they needed analytical data from their past utilization of Palantir software from the company in a format which was readable by their new software, which Palantir repeatedly refused to deliver, invoking intellectual property (Alden, 2017). Although it is unknown how this dispute ended, it nonetheless shows the potential problems associated with such platforms as they intervene deeply into the everyday police work such as knowledge creation and decision-making. As a current example of the dangers of the 'privatization of policing' through technologization, platformization shows that the use of technology by the police can always be accompanied by a loss of control and autonomy, which ultimately represents a risk for both the police and the citizens (Byrne and Marx, 2011: 31; see Privatization by Lomell).

Conclusion

The main take away points of this chapter are:

– Due to the increasing volume of data that organizations in general and police authorities in specific are exposed to, data integration and analysis platforms will become important tools in the day-to-day knowledge creation activities of police officers.

- By connecting heterogeneous data sources and dismantling boundaries between databases (desilozation), data integration and analysis platforms primarily aim to enhance interoperability.
- Data integration and analysis platforms intend to support and facilitate analytical actions by police officers, e.g., by showing associations between people in a visually convenient and actionable way.
- The approach of data integration and analysis platforms by definition is closely connected to issues of surveillance, since they aim to make as much data as possible accessible.
- Platformization provokes the reversion of an important civil rights principle: instead of checking a person more closely on the basis of concrete suspicion, people are now inspected via platforms to establish such a suspicion in the first place.
- Data integration and analysis platforms demonstrate once again the dangers of the privatization of policing through technologization, because they penetrate deep into the everyday work of police officers. This is ultimately linked to handing over a significant part of the knowledge generation to technologies and private companies and, thus, to the risk of losing autonomy and control.

Suggested reading

Brayne, S. (2021). *Predict and Surveil. Data, Discretion, and the Future of Policing.* Oxford: Oxford University Press.

Ferguson, A. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement.* New York: New York University Press.

Galis, V., & Karlsson, B. (2024). A world of Palantir – ontological politics in the Danish police's POL-INTEL. Information, Communication & Society, 1–19. https://doi.org/10.1080/1369118X.2024.2410255

Gundhus, H. O. I., & Wathne, C. T. (2024). Resistance to platformization: Palantir in the Norwegian police. *Information, Communication & Society*, online first, 1–19. https://doi.org/10.1080/1369118X.2024.2325533

Iliadis, A., & Acker, A. (2021). The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society*, 38(5), 334–363.

Ulbricht, L., & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society*, 11(3), 1–15. https://doi.org/10.1177/20539517241255108

References

Alden, W. (2017, June 28). *There's a fight brewing between the NYPD and Silicon Valley.* BuzzFeed News. https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley

Algorithm Watch. (2020). *Automating Society Report 2020.* https://automatingsociety.algorithmwatch.org

Anderson, C. (2008, June 23). The end of theory: The data deluge makes the scientific method obsolete. *Wired.* https://www.wired.com/2008/06/pb-theory/

Andersson Schwarz, J. (2017). Platform logic: An interdisciplinary approach to the platform-based economy. *Policy & Internet*, 9(4), 374 – 394. https://doi.org/10.1002/poi3.159

Atos. (2022). *Aufbau einer souveränen Recherche- und Analyseplattform für die Polizeien.* https://atos.net/wp-content/uploads/2022/09/WP-Aufbau-einer-souveraenen-Recherche-und-Analyseplattform-fuer-die-Polizeien.pdf

Bhuiyan, J. (2021). LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws. *The Guardian.* https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform

Biddle, S. (2017). *How Peter Thiel's Palantir Helped the NSA Spy on the Whole World.* The Intercept. https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/

Bigo, D. (2020). Interoperability: A political technology for the datafication of the field of EU internal security? In D. Bigo, T. Diez, E. Fanoulis, B. Rosamond, & Y. A. Stivachtis (eds.), *The Routledge Handbook of Critical European Studies* (pp. 400 – 417). London: Routledge. https://doi.org/10.4324/9780429491306

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, 82(5), 977 – 1008. https://doi.org/10.1177/0003122417725865

Brayne, S. (2021). *Predict and Surveil: Data, Discretion, and the Future of Policing.* Oxford: Oxford University Press.

Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. *Cahiers Politistudies*, 3(20), 17 – 40.

City of New Orleans. (2013). *NOLA for Life. Comprehensive Murder Reduction Strategy.* https://www.nola.gov/nola/media/Mayor-s-Office/Files/NOLA%20FOR%20LIFE/NOLA-FOR-LIFE-Sept2013-book-pdf_1.pdf

Egbert, S. (2019). Predictive policing and the platformization of police work. *Surveillance & Society*, 17(1/2), 83 – 88. https://doi.org/10.24908/ss.v17i1/2.12920

Eubanks, V. (2017). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* New York: St. Martin's Press.

European Parliament. (2020). *Answer given by Ms Johansson on behalf of the European Commission (9 June 2020).* https://www.europarl.europa.eu/RegData/questions/reponses_qe/2020/000173/P9_RE(2020)000173_EN.pdf

Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement.* New York: New York University Press.

Galis, V., & Karlsson, B. (2024). A world of Palantir – ontological politics in the Danish police's POL-INTEL. Information, Communication & Society, 1 – 19. https://doi.org/10.1080/1369118X.2024.2410255

Gates, K. (2019). Policing as digital platform. *Surveillance & Society*, 17(1/2), 63 – 68. https://doi.org/10.24908/ss.v17i1/2.12940

Gillespie, T. (2010). The politics of 'platforms'. *New Media & Society*, 12(3), 347 – 364. https://doi.org/10.1177/1461444809342738

Gundhus, H. O. I., & Wathne, C. T. (2024). Resistance to platformization: Palantir in the Norwegian police. *Information, Communication & Society*, online first, 1 – 19. https://doi.org/10.1080/1369118X.2024.2325533

Hardy, Q. (2016). The risk to civil liberties of fighting crime with big data. *The New York Times.* https://www.nytimes.com/2016/11/07/technology/the-risk-to-civil-liberties-of-fighting-crime-with-big-data.html

Hitachi Vantara. (2024). *Pentaho Data Integration and Analytics. Ingest, Integrate and Analyze.* https://www.hitachivantara.com/en-us/products/pentaho-plus-platform/data-integration-analytics.html

Iliadis, A., & Acker, A. (2022). The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society*, 38(5), 334 – 363. https://doi.org/10.1080/01972243.2022.2100851

KNIME. (2024). *KNIME Analytics Platform.* https://www.knime.com/knime-analytics-platform

Mason, R. (2023). Everything you need to know about NHS England's biggest ever IT contract. *The Guardian.* https://www.theguardian.com/society/2023/oct/12/everything-you-need-to-know-about-nhs-englands-biggest-ever-it-contract

Matak, V. (2021, August 2). *WFP and Palantir partner to tackle Covid-19 and world hunger* [Video]. World Food Programme (WFP). https://www.wfp.org/stories/video-wfp-and-palantir-partner-tackle-covid-19-and-world-hunger

McCue, C., & Parker, A. (2003). Connecting the dots: Data mining and predictive analytics in law enforcement and intelligence analysis. *The Police Chief*, 70(10), 115 – 122.

Palantir. (n.d.). *NOLA Murder Reduction. White Paper.* https://s3.documentcloud.org/documents/21032274/nola-murder-reduction-white-paper.pdf

Palantir. (2012). *Fighting Crime in Salt Lake City.* www.palantir.com/wp-assets/wp-content/uploads/2012/06/ImpactStudy_SLCPD.pdf

Palantir. (2020, November 12). Palantir is not a data company (Palantir Explained, #1) [Medium]. *Palantir Blog.* https://medium.com/palantir/palantir-is-not-a-data-company-palantir-explained-1-a6fcf8b3e4cb

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYU Law Review.* https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

Rola Security Solutions. (2024). *rsShadow. Shines a light in the darkness.* https://www.rola.com/en/rsshadow/

Uchida, C. D., Swatt, M., Gamero, D., Lope, J., Salazar, E., King, E., Maxey, R., Ong, N., Wagner, D., & White, M. D. (2012). *The Los Angeles Smart Policing Initiative: Reducing Gun-Related Violence through Operation LASER.* Los Angeles Police Department. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/losangelesspi.pdf

Ulbricht, L., & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society*, 11(3), 1 – 15. https://doi.org/10.1177/20539517241255108

van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media.* Oxford: Oxford University Press.

van Dijck, J., Poell, T., & de Waal, M. (2018). *The Platform Society: Public Values in a Connective World.* Oxford: Oxford University Press.

Wilson, D. (2019). Platform policing and the real-time cop. *Surveillance & Society*, 17(1/2), 69 – 75. https://doi.org/10.24908/ss.v17i1/2.12958

Wilson, D. (2021). The new platform policing. In A. Završnik & V. Badalič (eds.), *Automating Crime Prevention, Surveillance, and Military Operations* (pp. 47 – 68). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-73276-9_3

Wood, S. E. (2019). Policing through platform. *Computational Culture*, 7 (21 October 2019). http://computationalculture.net/policing-through-platform/