Anthony Amicelle

28 Financial crime and surveillance

Abstract: This chapter aims at presenting and questioning the main follow-the-money techniques in digital societies for crime-control and national security purposes. It shows how national and transnational policing configurations increasingly rely on digitized financial surveillance, mainly practiced by and within leading capitalist institutions that are not proper private security companies.

Keywords: algorithm, capitalism, policing, suspicion, transnational

Introduction

“I would say, ‘Follow the money, Earl, because that’s where it’s going to be’. Unfortunately, we did not get it following the money because the records were either nonexistent or were destroyed.” This sentence is generally considered as the first ever official occurrence of the catchphrase ‘follow the money.’ It was pronounced by the Assistant Attorney General of the Nixon administration in June 1974, during the US Senate committee hearings on the nomination of Earl J. Silbert, the first prosecutor in the Watergate scandal. The expression was eventually popularized two years later by *All the President’s Men*, the award-winning movie based on Carl Bernstein and Bob Woodward’s bestseller. Today, according to international norms and criminal laws, financial flows must be—and are more and more—constantly monitored and traced to detect and prosecute a wide range of criminal activities, whilst identifying and tracking terrorists and preventing the proliferation of weapons of mass destruction. Despite differences in scale and approach, financial surveillance systems share two critical commonalities. On the one hand, financial surveillance is largely mediated by digital technologies, from algorithmic devices for suspicion to mass dataveillance schemes for collecting bulk data from commercial databases (see Surveillance by Lyon). On the other hand, the operation of highly digitized financial surveillance primarily depends on the involvement of social actors and institutions who are neither public police and intelligence services, nor proper private security companies.

Follow the money in digital societies

“In a globalized world where technology allows money to move quickly anywhere, fighting money laundering is more urgent than ever. Trillions of dollars are laundered each year. That money fuels serious crime. #FollowTheMoney.” This is an excerpt of the public campaign launched by the Financial Action Task Force, namely the international policy-making body against illicit financial flows (Nance, 2018). Initiated in 1989, this global policy is now formally applied in more than 200 countries and jurisdictions, whilst covering any kind of dirty money-related crime, from petty theft to major illegal traffickings and ruling elites illegalities, as well as terrorism and proliferation financing (Levi, 2010; Amicelle and Chaudieu, 2022). In practice, it translates into everyday financial surveillance, first and foremost to spot and report suspicious transactions for public safety and national security purposes (Harvey and Lau, 2009). But what are 'suspicious transactions,' who 'follows the money,' and how in the so-called high-tech globalized world?

Financial surveillance for crime control is conducted by corporations, starting with banks as "reluctant partners" enlisted to monitor what they are intended to circulate (Favarel-Garrigues et al., 2011; Bosma, 2022). More broadly, such a legally binding vigilance is "part of a security chain, whereby commercial data are analysed, collected, reported, shared, moved, and eventually deployed as a basis for intervention by police and prosecution. In this context, private companies – including Facebook and Twitter, airlines and banks – find themselves in the frontline of fighting terrorism and other security threats" (de Goede, 2018: 25). Policing and security configurations increasingly rely on such pillars of capitalism that are not strictly speaking private security companies, including financial institutions as well as social media platforms (Crosset and Dupont, 2022), cross-border logistics and transport businesses (Nøkleberg, 2022; Glouftsios and Leese, 2023). Unlike for-profit providers of security services and technologies of which they are themselves clients, high and low policing is neither their core business nor a direct source of capital accumulation. They do not fit the canon of the private police, referring to "the various lawful forms of organized, for-profit personnel services whose primary objectives include the control of crime, the protection of property and life, and the maintenance of order" (Joh, 2004: 55). They are originally positioned in economic and financial fields distinct from the transnational field of security at large, and the related struggles over the legitimate definition, classification, and management of internal and external security threats (Bigo, 2008).

From this perspective, both state surveillance in the name of security and corporate surveillance in the name of financial gain, especially in the age of surveillance capitalism (Zuboff, 2019), are well identified phenomena in public debate. "But the fact that the government and private establishments can participate together in 'surveillant assemblages' in the name of common objectives escapes [or at least has escaped for a long time] an analytical framework in which state and commercial purposes in collecting personal information seem incompatible" (Amicelle and Favarel-Garrigues, 2012: 117). Banks are still almost exclusively seen as organizations where we can invest or borrow money, and not as eyes and ears of the security state in the financial space, echoing public campaigns urging anyone to report suspicious activities 'if they see something' (Reeves, 2017). While they remain financial services providers on behalf of their clients, banks have also become surveillance and informant bodies on behalf of law enforcement and intelligence agencies, with up to tens of millions of financial transactions reports annually in some western countries, including several hundreds of thousands of suspicious transactions reports.

To do so, financial surveillance operates in several ways, from face-to-face surveillance to big dataveillance at a distance, with a strong emphasis on the widespread but ambivalent use of algorithmic systems (see Algorithms by Leese).

First of all, part of surveillance is still conducted ‘over-the-counter,’ in bank branches where clients can show up for financial operations. As part of anti-money laundering/countering the financing of terrorism compliance, banking staff, from tellers to wealth managers, must be trained to detect unusual and suspicious activities when in contact with customers (Favarel-Garrigues et al., 2008; Iafolla, 2018). In this context, surveillance is mainly focused on people’s interactional behavior, in light of “potential red flags” provided by State authorities, such as “client exhibits nervous behaviour” (Amicelle, 2022). Each internal alert is then processed by banks’ dedicated analysts to determine whether it must be reported to the State competent authority, namely the national financial intelligence unit (Lagerwaard, 2023; Amicelle, 2020).

Secondly, financial surveillance is also conducted on the basis of risk scoring. This leads to “stratified surveillance: differentially surveilling individuals according to their [dirty money] risk score” (Brayne, 2017: 989). Unlike face-to-face surveillance in bank branches, risk-based surveillance is conducted at a distance, without any direct interaction and observation of clients whose financial operations are placed under enhanced monitoring. The latter is carried out manually through regular reviews of high-risk clients’ transactions and capital movements on the basis of recorded digital trails. The aim is still the same, i. e., to detect unusual and suspicious activities, but this time in light of transactional behaviour, with “potential red flags” such as “the transactional activity (level or volume) is inconsistent with the client’s apparent financial standing, their usual pattern of activities or occupational information (e. g. student, unemployed, social assistance, etc.)” (Amicelle and Iafolla, 2018).

Over the last years, both of these forms of financial surveillance have been deemed insufficient to comply with new requirements of permanent and systematic transactions monitoring. On the one hand, surveillance over-the-counter is by definition discontinuous and partial. It only occurs during occasional interactions, which additionally become increasingly rare because of the steady decline of the number of client visits in bank branches. On the other hand, risk-based surveillance at a distance is also limited to the extent that it targets roughly 1% of the banking population, i. e., the high-risk scored clients. In this context, algorithmic devices have gradually become critical actants of financial surveillance for crime control (Amicelle and Grondin, 2021), to make a difference in three, interrelated ways.

First of all, they are deployed to monitor everyone’s transactions at any time, whether or not we show up in bank branches, and regardless of our risk score. Second, they contribute to the predominance of transactional dataveillance. Indeed, transactional metrics and relations come first, and may be self-sufficient to create alerts, without any necessary reference to clients’ socio-demographic and financial profile. Finally, the operation of surveillance and related creation of alerts are therefore automated, and no longer manual as compared with previous—and still coexisting—financial surveillance systems. Nevertheless, human intervention and decision-making processes do not vanish altogether, as in most configurations of algorithmic policing and security, from police patrols to penal courts (Benbouzid, 2019; Brayne and Christin, 2021), criminal intelligence and transnational security apparatuses (Chan and Bennett Moses, 2017; Bigo and Bonelli, 2019). Algorithmic devices are designed as 'recommender systems' for agents whose responsibility is to analyze each automated alert whilst undertaking additional verification before making any final decision (Bellanova and de Goede, 2022).

In light of the growing interdisciplinary literature on algorithmic systems for policing, intelligence, and security at large, their widespread use in financial surveillance does not come as a surprise. But their relative simplicity does, by contrast with public discourses and theoretical if not speculative studies about artificial intelligence security technology. To date, the so-called big data financial surveillance programs are based on quite basic if-then commands with predefined sets of actions, far from what Daniel Neyland critically depicts as the "the algorithmic drama in current academic research" (Neyland, 2019: 81). This reflects the structural tension of crime control configurations based on the interconnection of differentiated universes of practices and rationalities, from finance to economic regulation and security intelligence. In the end, this does give rise to automated and everyday mass financial surveillance whilst remaining far removed from crime-control ambitions as it is from dystopian visions of big data, with minimal consequences if any on the existing financial order (Amicelle, 2022). In addition to the global policy against 'dirty money' that covers both money laundering and terrorist financing, the prioritization of this last issue in the context of the War on Terror has also given rise to another specific form of mass financial surveillance.

Transnational financial dataveillance in the name of counter-terrorism

"By following the money, the TFTP has allowed the U.S. and our allies to identify and locate operatives and their financiers, chart terrorist networks, and help keep money out of their hands." This is one of the current official US Treasury's promotion of their Terrorist Finance Tracking Program (TFTP), launched in October 2001 while only—and controversially—unveiled in the media in June 2006 (Gonzalez Fuster et al., 2008; Amicelle, 2011; Wesseling et al., 2012). As the most important financial data-driven surveillance programs for national security purposes, the condition for the possibility of the TFTP to exist can be summed up in a single word: traceability. According to Hermitte, "surveillance, an old reality, only becomes the modern traceability when it is carried out within an organised system, the extent of which suggests that it is a genuine project for society, pursued as much by private as by public authorities" (Hermitte, 2003: 3). Regarding transnational financial flows, such an organized system of traceability has first been implemented by the Society for Worldwide Interbank Financial Telecommunication—SWIFT, the self-defined backbone of global financial communication—and then by the US administration in the name of the War on Terror.

"To speak of traceability involves bringing together three elements: there must be traces and therefore a medium that makes it possible to locate them; there must be a mechanism for collecting these traces; and finally there must be a structure that allows them to be processed and analysed in order to draw conclusions. Without this type of organisation, which implies a more or less assertive voluntarism, traces do in fact exist, but not 'traceability'" (Hermitte, 2003). The SWIFT messaging platform is used by 11,000 financial institutions in more than 200 hundred countries and territories to channel up to 80 % of the digital value transfers around the world, with over 40 million messages a day, for more than 8 billion messages in 2023. In this context, financial traceability has been organized by SWIFT for commercial purposes. Each message generates digital traces that are temporarily collected and stored in SWIFT data centers, with a socio-technical structure to search and analyze them if needed. In case of unexpected problem or any specific demand from financial institutions, the cooperative is then able to find digital trails in relation to channeled transnational transactions. All three elements of traceability are thus combined for quality of the systemic messaging service.

In October 2001, this commercially organized system of traceability intersected with the US administration aim of a national security organized system of traceability, i. e., the Terrorist finance tracking program on the basis of a secondary use of SWIFT messages digital trails (Amicelle, 2013; de Goede and Wesseling, 2017). The issue of secondary use "involves data collected for one purpose being used for an unrelated purpose without people's consent" (Solove, 2007: 770). US Treasury officials have justified the access and processing of bulk data from considerable number of SWIFT messages to preemptively disrupt and incapacitate terrorist suspects. More precisely, two main narratives have been used to promote the added-value of the TFTP-related financial surveillance.

On the one hand, as other security programs with dataveillance capabilities, the TFTP has been promoted in light of interconnecting mobilities, from tracing digitized financial mobilities to finding and following physical traces of human mobilities. According to oft repeated official discourses, "For example, it is possible to locate a suspect by checking when and where the suspect closed and/or opened a new bank account in a city or country other than his or her last known place of residence. This is a clear indicator that the person may have moved. […] The terrorist finance tracking program can provide key information about the movements of suspected terrorists and the nature of their expenditures" (EU Commision, 2013: 5). In other words, on the basis of digital financial trails, the added-value would be to trace back money flows to geographically track terrorist suspects. On the other hand, it has been officially promoted to map terrorist networks. As Marieke de Goede (2012) critically points out, financial connectivity is presented as the glue or binder that holds a whole terrorist network together and as such is believed to be a major source of intelligence. This primacy given to financial relations produces suspicion by association. Having sent or received money from a known terrorist suspect casts doubts if not outright suspicions about the individual involved.

Although the efficiency and regulation—through EU–US agreements (Bellanova and de Goede, 2022)—of such a mass financial surveillance program is still a matter of major debate in terms of privacy and fundamental rights (see Privacy and Data Protection by Bygrave), information asymmetry between sovereign entities, lack of preemptive effectiveness, and questionable added value at large, the terrorist finance tracking program has continued to exist since 2001, almost the beginning of the 21st century.

Conclusion

For the last decades, 'follow the money' has thus become the official motto of the main global policy of crime control, and the underlying logic of one of the most important transnational counter-terrorism program to date. If policing refers to "the creation of systems of surveillance coupled with the threat of sanction for deviance – either immediately or by initiating penal processes" (Reiner, 2010: 5), then what is specific to contemporary policing is the increasing significance of financial surveillance systems.

- National and transnational policing configurations increasingly rely on digitized financial surveillance.
- Financial surveillance is practiced by and within leading capitalist companies, whose economic rationale is, at first sight, relatively far from criminal law and security interventions.
- The State collection, storage, and processing of large amounts of digital data at the core of global finance functioning is used to inform national security decisions.

From this perspective, *financial surveillance: who cares?* (Amicelle and Favarel-Garrigues, 2012) should no longer be a relevant research question.

Suggested reading

Amicelle, A. (2022). Big data surveillance across fields. Algorithmic governance for policing and regulation. *Big Data & Society*, 9(2).

De Goede, M. (2012). *Speculative Security: The Politics of Pursuing Terrorist Monies.* Minneapolis: University of Minnesota Press.

King, C., Walker, C., & Gurule, J. (eds.) (2018). *The Palgrave Handbook of Criminal and Terrorism Financing Law.* Cham: Palgrave Macmillan.

References

Amicelle, A. (2011). The great (data) bank robbery: The terrorist finance tracking program & the 'SWIFT Affair', *Research Questions*, 36, 1 – 27.

Amicelle, A. (2013). The EU's paradoxical efforts at tracking the financing of terrorism. From criticism to imitation of dataveillance. *Liberty and Security Series*, 56, 1 – 19.

Amicelle, A. (2020). Right of entry. The struggle over recognition in the world of intelligence. *Political Anthropological Research on International Social Sciences*, 1(2), 243 – 272.

Amicelle, A. (2022). Big data surveillance across fields. Algorithmic governance for policing and regulation. *Big Data & Society*, 9(2).

Amicelle, A., & Chaudieu, K. (2022). The most denounced, the least punished: Ruling elites, illegalisms and anti-money laundering. *International Political Sociology*, 16(3), 1 – 22.

Amicelle, A., & Favarel-Garrigues, G. (2012). Financial surveillance: Who cares? *Journal of Cultural Economy*, 5(1), 105 – 124.

Amicelle, A., & Grondin, D. (2021). Algorithms as suspecting machines: Financial surveillance for security intelligence. In D. Lyon & D. Murakami Wood (eds.), *Big Data Surveillance and Security Intelligence: The Canadian Case* (pp. 68 – 87). Vancouver: University of British Columbia Press.

Amicelle, A., & Iafolla, V. (2018). Suspicion-in-the-making: Surveillance and denunciation in financial policing. *The British Journal of Criminology*, 58(4), 845 – 863.

Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, 16(1), 102 – 118.

Benbouzid, B. (2019). To predict and to manage. Predictive policing in the United States. *Big Data & Society*, 6(1).

Bigo, D. (2008). Globalized (in)security: The field and the ban-opticon. In D. Bigo and A. Tsoukala (eds.), *Terror, Insecurity and Liberty* (pp. 10 – 48). London: Routledge.

Bigo, D., & Bonelli, L. (2019). Digital data and the transnational intelligence space. In D. Bigo, E. Isin, & E. Ruppert (eds.), *Data Politics: Worlds, Subjects, Rights* (pp. 100 – 122). London: Routledge.

Bosma, E. (2022). *Banks as security actors: Countering terrorist financing at the human-technology interface.* [Thesis, fully internal, Universiteit van Amsterdam].

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

Brayne, S., & Christin, A. (2021). Technologies of crime prediction. *Social Problems*, 68(3), 608 – 624.

Chan, J., & Bennett Moses, L. (2017). Making sense of big data for security. *The British Journal of Criminology*, 57(2), 299 – 319.

Crosset, V., & Dupont, B. (2022). Cognitive assemblages: The entangled nature of algorithmic content moderation. *Big Data & Society*, 9(2).

de Goede, M. (2012). Fighting the network: A critique of the network as a security technology. *Distinktion*, 13(3), 215 – 232.

de Goede, M. (2018). The chain of security. *Review of International Studies*, 44(1), 24 – 42.

de Goede, M., & Wesseling, M. (2017). Secrecy and security in transatlantic terrorism finance tracking. *Journal of European Integration*, 39(3), 253 – 269.

European Commission. (2013). *Joint Report from the Commission and the U.S. Treasury Department regarding the Value of TFTP Provided Data.* Brussels.

Favarel-Garrigues, G., Godefroy, T., & Lascoumes, P. (2008). Sentinels in the banking industry: Private actors and the fight against money laundering in France. *The British Journal of Criminology*, 48, 1 – 19.

Favarel-Garrigues, G., Godefroy, T., & Lascoumes, P. (2011). Reluctant partners? Banks in the fight against money laundering and terrorism financing in France. *Security Dialogue*, 42(2), 179 – 196.

Gonzalez Fuster, G., De Hert, P., & Gutwirth, S. (2008). SWIFT and the vulnerability of transatlantic data transfers. *International Review of Law Computers & Technology*, 22(1 – 2), 191 – 202.

Glouftsios, G., & Leese, M. (2023). Epistemic fusion: Passenger Information Units and the making of international security. *Review of International Studies*, 49(1), 125 – 142.

Harvey, J., & Lau, S. F. (2009). Crime-money, reputation and reporting. *Crime, Law and Social Change*, 52, 57 – 72.

Hermitte, M.-A. (2003). La traçabilité des personnes et des choses. Précaution, pouvoirs et maîtrise. In P. Pedrot (ed.), *Traçabilité et responsabilité* (pp. 1 – 44). Paris: Economica.

Iafolla, V. (2018). The production of suspicion in retail banking: An examination of unusual transaction reporting. In C. King, C. Walker, & J. Gurule (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 81 – 107). Cham: Palgrave Macmillan.

Joh, E. E. (2004). The paradox of private policing. *The Journal of Criminal Law and Criminology*, 95(1), 49 – 131.

Lagerwaard, P. (2023). Financial surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands. *Journal of Money Laundering Control*, 26(7), 63 – 84.

Levi, M. (2010). Combating the financing of terrorism. A history and assessment of the control of 'threat finance'. *The British Journal of Criminology*, 50(4), 650 – 669.

Nance, M. T. (2018). The regime that FATF built: An introduction to the financial action task force. *Crime, Law and Social Change*, 69(2), 109 – 129.

Neyland, D. (2019). *The Everyday Life of an Algorithm.* New York: Palgrave Macmillan

Nøkleberg, M. (2022). Expecting the exceptional in the everyday: Policing global transportation hubs. *Security Dialogue*, 53(2), 164 – 181.

Reeves, J. (2017). *Citizen Spies. The Long Rise of America's Surveillance Society.* New York: New York University Press.

Reiner, R. (2010). *The Politics of the Police, 4th ed.* Oxford: Oxford University Press.

Solove, D. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, 44, 745 – 772.

Wesseling, M., De Goede, M., & Amoore, L. (2012). Data wars beyond surveillance: Opening the black box of SWIFT. *Journal of Cultural Economy*, 5(1), 49 – 66.

Zuboff, S. (2019). *The Age of Surveillance Capitalism.* New York: PublicAffairs.