Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy

*Valeria Ferrari**

Financial data are key to various law enforcement processes, including criminal investigations, anti-money laundering strategies and the implementation of national fiscal policies. However, financial data also qualify as personal data. While law enforcement objectives can derogate certain privacy-related legal safeguards, private financial firms should, in principle, comply with the privacy standards upheld by GDPR. Highlighting the most critical trends of the current financial industry (i.e. commercial exploitation of data; international dimension of financial informational networks; use of automated processing and decision-making tools), the present paper analyses how privacy and law enforcement priorities interplay in determining the governance of financial data. We conclude by recognizing that privacy loopholes exist in the current financial industry's data practices, and that - as payments tend to be increasingly performed in digital manners, exponentially increasing the availability of financial data - privacy-enhancing payment methods should be encouraged and legitimised.

Keywords: Financial data | law enforcement | data economy | privacy

I. Introduction

Data regarding financial transactions are a crucial source of information for law enforcement. Financial transactions' data can signal illicit activities such as tax evasion, money laundering and terrorist financing. Triangulated with other personal datapoints, they allow to infer information about individuals' activities, purchases and geographical movements, from which, in turn, sexual orientation, health status, religious and political beliefs and cultural preferences can be derived.

Events such as the 2008 financial crisis and the 9/11 terrorist attack constituted the premises for a public discourse that puts the enhanced transparency and securitisation of finance among the top priorities of regulatory agendas. Regulatory updates in the European legal frameworks have strengthen the requirements for customer identification, recordkeeping and data retention for activities involving the transfer and storage of funds. Legal measures have also been taken to prevent wealth from bypassing national fiscal policies by flowing into offshore financial centres. Bank secrecy has been undermined even in previously established fiscal havens.

The concrete implementation of these policy goals depends, ultimately, on the capillarity of public-private informational networks, which vary among geographical areas and business types.

In the same period of time, another legal priority - also aimed at increasing the trustworthiness of powerful intermediaries - has been pursued by European regulators: privacy. The adoption of the General Data Protection Regulation (GDPR)[1] enhances efforts in granting individuals specific legal rights regarding their own personal data, to be guaranteed by any kind of commercial entity that collects such data for its business purposes.

DOI: 10.21552/edpl/2020/4/8

* PhD candidate at the Institute for Information Law, University of Amsterdam. Research fellow at Weizenbaum-Institut, Berlin. For correspondence: <v.ferrari@uva.nl>

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

On one side, European regulatory updates on Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies and tax administration law demand financial institutions extensive collection and storage of personal data. Moreover, the Payment Service Directive 2 (PSD2)[2] obliges financial institutions to share data with Third Party Providers to facilitate the functioning and competitiveness of European payment markets. On the other side, the GDPR imposes on information intermediaries the principle of data minimization and grants individuals' the right to have their data rectified, erased or transferred according to their will. Financial institutions, therefore, are expected to enforce legal requirements and policy goals that are uneasy to incorporate within the same technological and governance structure.

As the modality of the practical, mutual integration of these coexisting legal frameworks is not clearly spelled out by the legal frameworks themselves, their concrete co-applicability is often shaped by financial intermediaries' industry standards.[3] Automated tools for data processing and bulk collection of personal data are incentivised by law enforcement legal requirements. Moved by efficiency and risk considerations, industry actors minimize their legal liabilities by automating their compliance procedures through technical means of data collection, analysis and elaboration.[4] At the same time - as private financial intermediaries are moved by commercial incentives - data are involved in channels of commercial exploitation. The resulting technological standards and data practices are oftentimes debatable from a privacy point of view, so that it becomes fundamental to scrutinise which actors, and which interests, determine the governance of financial informational networks.

This paper illustrates emerging privacy and data protection issues that derive from the digitalisation of the financial infrastructure. The view underlying this study is that the coexistence of privacy and law enforcement legitimate interests requires to admit spaces where one or the other goal is sacrificed for the benefit of the other. Physical cash traditionally circumscribes one of these spaces, as it allows untraceable transactions preserving privacy at the expense of enforcement capabilities. The digitalization of the payment infrastructure and the gradual disappearance of cash, however, is leading to a situation of perfect enforcement: even when small-scale transactions are concerned, the financial digital architecture does not admit 'weak spots' where transactions are not associated with individuals and interlinked with other pieces of information.

Recognising both privacy and prevention/investigation of illegal activities as legitimate policy goals, this study suggests that regulators should seek for institutional arrangements that - while not giving up public interest and security objectives - safeguard financial data from the plurality of surveillance networks expanding in this area. This implies favouring 'imperfect' over 'perfect' enforcement - conceding, by remotion, legitimate spaces for privacy in financial transactions.

Section II defines the problem by (1) circumscribing the concept of "financial data"; (2) illustrating the role of such data in law enforcement and public administration processes; and (3) exposing the data protection normative framework that applies to the processing of financial data. Hence, privacy issues in the financial domain are further scrutinised in light of the most recent industry developments (Section III). Finally, Section IV presents some concluding normative considerations, suggesting legal and technical paths that can be explored to enhance privacy and data protection in financial information networks. Identifying an important direction for future research, the paper encourages the promotion – from the part of policymakers - of techno-institutional arrangements for privacy-enhancing digital payment tools.

II. II. Financial Data Between Law Enforcement Priorities and Privacy Considerations

1. Definition of 'Financial Data'

Neither legal frameworks regarding data collection and retention for law enforcement purposes, nor pri-

2 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

3 Michelle Frasher, Brian Agnew, 'Multinational banking and conflicts among US-EU AML/CTF compliance & privacy law: operational & political views in context', (2016) Swift Institute Working Paper No. 2014-008.

4 ibid

vacy legal instruments identify a notion of 'financial data'. The present paper, consistently with this approach, refers to 'financial data' without suggesting the existence of a sui generis kind of data generated in the context of financial activities. Rather, the term 'financial data' is used, for the purpose of this paper, to refer to data that (a) is linked to an individual or more individuals (data subject); and that is either (b)(i) directly tied to a financial account, transaction or customer's credit profile (data type); or (ii) involved in a financial process (data use).[5] This definition is practical as it allows to narrow the scope of the study without relying on the identification of the legal entity involved in the transaction, and without differentiating between personal data based on the use (commercial or law enforcement) that is made of it.

Different kinds of personal data are involved in financial activities. Data that is strictly related to financial transactions can be referred to as 'transactional data', i.e. the amount of funds transferred from x to y. The PSD2 identifies the category of 'sensitive payment data', defined as 'data, including personalised security credentials which can be used to carry out fraud'[6] – e.g. credit cards' numbers and security codes. However, financial intermediation implies the transmission, storage and elaboration of a wide variety of personal information that go well beyond the mere recording of transactions' values and accounts' identifiers. Personal data is collected (and acquired from third party service providers) and used by financial firms for multiple reasons, which can broadly be categories as (a) performance of the service as specified by the contract between the service provider and the costumer; (b) user profiling for marketing purpose; or (c) legal compliance obligations.

The aggregation and analysis of transactional data with other personal identifiable information and the prolonged observation of patterns in financial activities serve to the creation of datasets which we can define as 'derivative' data. This category of triangulated, elaborated data often constitutes the information that financial intermediaries hand over to law enforcement agencies and to various third parties to build customer profiles for credit risk analysis. The sub-derivative data which constitutes profiling is, furthermore, involved in automated decision-making processes and used to build intelligence and marketing strategies.

2. The Role of Financial Data in Law Enforcement

The traditional study of politics by Harold Lasswell (1936) locates information among the resources that are key to the art of 'statecraft'.[7] The government of modern societies is organized around knowledge. Sovereign states need data about citizens to administrate the wealth and behaviours of large population.[8] The collection, sorting, organization and analysis of massive amounts of data are fundamental to large-scale political economies. Data-based administration is thus the prominent form in which (political, social, economic) power manifests itself and is exercised in modern society.

Financial records are particularly crucial for law enforcement processes. The administration of welfare policies largely depends on government's' ability to access financial databases and records of both individuals and businesses transactions.[9] Abolishing anonymity is the primary step to eradicate welfare fraud and to detect criminal undertakings. Centralized firms and institutions are entrusted to gather, access and manipulate the information that is necessary to protect the security and correct functioning of the financial system. Forms of 'information mercantilism'[10] have long tied together law enforcement apparatuses and financial firms. Managing wealth in the form of credit and debt recording, financial intermediaries operate in liaison with administrative agencies and cover roles that some political econo-

5 Marshall Lux, Matthew Shackelford, 'The new frontier of consumer protection: financial data privacy and security', (2020) M-RCBG associate Working Papers Series No. 135 <https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/Lux_Final_March2020.pdf> accessed 10 June 2020.

6 Art 4(32) PSD2.

7 Harold Lasswell, *Politics: Who Gets What, When*, How (Cleveland/New York 1936).

8 Michel Foucault, 'Governmentality' in *The Foucault Effect: Studies In Governmentality* (1991) edited by G. Burchell, C. Gordon, Miller, 87–104, University Of Chicago Press.

9 See also: Theodore M Porter, *Trust In Numbers* (Princeton: Princeton University Press, 1996); James C. Scott, *Seeing Like A State: How Certain Schemes To Improve The Human Condition Have Failed* (New Haven: Yale University Press, 1998); Josh Lauer, *Creditworthy: A History Of Consumer Surveillance And Financial Identity In America* (Columbia University Press, 2017).

10 Eric Rosenbach, Katherine Mansted, 'The Geopolitics Of Information', (2019) Belfer Center For Science And International Affairs <https://Www.Belfercenter.Org/Publication/Geopolitics-Information> last accessed 10 June 2020.

mists have targeted as quasi-public.[11] Financial information agents, therefore, are responsible not only for the economic stability of a monetary system, but also for the trustworthiness of administrative and judicial processes.

Demands for greater transparency, better record-keeping and oversight of financial information channels have increased steeply in the aftermath of the 2008 financial crisis.[12] In the EU, legislative frameworks have been updated to enhance the pressure on financial institutions to share data with other financial institutions, government agencies and international bodies.[13] The 5th Anti-Money Laundering Directive (5thAMLD)[14] and other legal instruments[15] mandate that financial intermediaries have in place automated systems for customer identification, transactions monitoring and reporting. These compliance processes imply massive data collection, long data retention periods and the use of automated tools for suspicious transactions' detection and red flagging.

The digitalisation of monetary flows allows to organise capillary systems of financial surveillance that exceed previously conceivable levels of efficiency. Following the logics of actuarial justice and risk-based regulation, individuals and groups are subjected to automated profiling and decision-making.[16] An extensive legal doctrine discusses the normative issues associated with data-driven, automated decision-making.[17] These issues not only concern privacy and individual autonomy, but also the erosion of the principles of due process, fairness and equality. Thus, it becomes necessary to define clear boundaries within which efficiency gains can be advanced at the expense of privacy and fundamental rights.

Surveillance-based enforcement networks built around financial databases must be scrutinised both for their dimension and pervasiveness, and for the interests that are involved in their construction and maintenance. The extensive reliance on private intermediaries raises the question of whether these parties are worthy of the trust that enforcement duties imply.[18] As events in 2008 demonstrated, the self-interest of private parties is not always aligned with public interest. The over reliance on financial firms for maintaining the edifice of risk management determined a collapse of the system. Similarly, entrusting financial corporations with the task of balancing the safety and the privacy of citizens might lead to disappointing outcomes.

Financial entities are not immune to the economic incentives that inform data practices in other industries. Ubiquitous data gathering, required for capillary enforcement, feeds into the logic of accumulation typical of 'surveillance capitalism'.[19] Data becomes a new asset and firms acquire economic power by 'channelling and controlling flows of personal information'[20]. The other face of financial surveillance is, in other words, the emergence of business models that exploit personal information in ways that are often opaque to both individuals and public authorities.[21]

11 See: Robert E. Litan, Michael Pomerleano, Vasudevan Sundararajan, *Financial sector governance: the roles of the public and private sectors* (Brookings Institution Press, 2002); W. Travis Selmier II, Michelle Frasher, 'The Cross-Atlantic tussle over financial data and privacy rights', (2013) Business Horizons 56, 767-778.

12 On the linkages between financial crises and weak spots in financial informational networks, see: Malcolm Campbell-Verduyn, Marcel Goguen, Tony Porter 'Finding Fault Lines In Long Chains Of Financial Information' (2019) Review of International Political Economy.

13 For an overview of the actions undertaken in the context of European financial reform, visit: <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-reforms-and-their-progress/progress-financial-reforms_en> last accessed 15th October 2020.

14 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 may 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (AMLD).

15 eg Directive (Eu) 2015/2366, Directive 2006/24/Ec, etc.

16 See: Mireille Hildebrandt, 'Profiling and AML' (2009) in Kai Rannenberg, Denis Royer, Andre Deuker, '*The Future of Identity in the Information Society. Challenges and Opportunities'* (Springer, 2009).

17 See: Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation'(2017), Regulation and Governance 12(4); Maayan Pere, Niva Elkin-Koren, 'Black box tinkering: beyond disclosure in algorithmic enforcement', *Florida Law Review* 69(181); Frank Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information* (Harvard, 2015).

18 Balázs Bodó, 'Mediated Trust – A Theoretical Framework to Address the Trustworthiness of Technological Trust Mediators' (2019) <https://ssrn.com/abstract=3460903> or <http://dx.doi.org/10.2139/ssrn.3460903> last accessed 10th June 2020.

19 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Publicaffairs, 2019).

20 Yeung (n 18) 20.

21 This phenomenon can be read as tendency toward the 'platformisation' of the industry; see: Nick Srnicek, *Platform capitalism* (Polity, 2017).

3. Financial Data and Data Protection Normative Frameworks: A Double Standard?

Financial information is processed and stored by private financial intermediaries in the pursue of, primarily, commercial interests. The GDPR applies when personal data is processed by commercial entities established within the Union, or when such data refers to subjects located in the EU.[22] In relation to such processing, the regulation establishes rules and principles aimed at protecting individuals against unfair uses of their personal information. It spells out clear responsibilities for so called 'data controllers'[23] and 'data processors'[24], including obligations to grant individuals' a series of rights regarding personal data related to them.

Financial firms' data processing practices are, however, also deeply connected to administration and law enforcement mechanisms. Hence, the data they manage has a dual use and sits in a grey area of data protection. When the legal basis for data processing is the performance of law enforcement-related operations, in fact, the standard GDPR regime gives way to other provisions aimed at balancing data protection legal safeguards with the needs of law enforcement agencies.

The GDPR provision that opens the possibility for law enforcement-related derogations is Article 23. Such Article provides that EU or national law may restrict the scope of the obligations and rights established by the Regulation for reasons of public security, for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and to pursue 'other important objectives of general public interest' including 'monetary, budgetary and taxation a matters, public health and social security'.[25] The conditions for such restrictions to be admissible within the GDPR framework are that they are provided by law, that they do not interfere with fundamental rights and are necessary and proportionate in a democratic society.[26]

Financial information is, indeed, in multiple cases used for the purposes listed in Article 23. This is foreseen by Recital 112, whereas it specifies that 'derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities'.

When law enforcement duties allow private entities to derogate from the their GDPR obligations, however, data processing does not take place in a legal vacuum: the regime governing data processing for non-commercial purposes must be found elsewhere. The so-called Law Enforcement Directive (LED)[27] has been adopted to cover what the GDPR had left out: the protection of data that are processed for law enforcement purposes. It applies to a) public authorities processing data for the purposes of preventing, investigating, detecting or prosecuting of criminal offences, or for safeguarding public security; and b) any other entity entrusted by national law to process data for the above-mentioned law enforcement objectives.[28] Seeking to establish a level playing field across the EU on law enforcement cooperation and related data protection standards, the legal instrument demands national policymakers to define the appropriate rules to achieve the stated goals.

Notwithstanding the proposition of GDPR-inspired principles, the LED demonstrates the difficulty of balancing privacy with law enforcement priorities. On one side, it values the idea of individual controllership and transparency. On the other, it foresees law enforcement as the only legal basis for processing, excluding by default the need – or even the possibility – of consent.[29]

While the legal instrument lists a number of data subject rights (information, data access, rectification and erasure rights) it also leaves wide possibilities for national provisions to limit them. Indeed, it's hard to imagine how – for instance, in the context of crim-

22 Art 3 GDPR.

23 Art 24 GDPR.

24 Art 28 GDPR.

25 Art 23(1) GDPR.

26 ibid

27 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89.

28 Art 3(7) LED.

29 Mark Leiser, Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', (2019) European Data Protection Law Review 5(3).

inal investigations – data subjects could exercise their rights without compromising the effectiveness of law enforcement activities. Therefore, the possible obstruction of law enforcement processes is foreseen as a justification for denying information or access rights. Similarly, data rectification or erasure claims can be dismissed if the concerned data serves as judicial evidence[30]. As it concerns financial data, such eventuality presents itself in the context of AML procedures. According to the 5thAMLD, Member States can impose up to seven years of data retention for AML purposes, even after a customer's account has been closed.[31] This will eventually override data subjects' right of erasure.

In short, it can be said that different legal regimes apply when data is processed for commercial purposes or for law enforcement ones. This double standard becomes problematic when law enforcement data processing is performed – as it often happens when financial data is concerned – by private firms. In fact, data that is collected for economic purposes could then be exploited in the context of legal inquiries or used as evidence. It can be impractical to determine when one regime should give way to the other, and data subjects can see the GDPR legal protections decrease or vanish when a law enforcement procedure involving their data is initiated.

The resulting situation is one of legal uncertainty that threats to undermine the principle of purpose limitation. This has been underlined by the Article 29 Data Protection Working Party (WP29), in its 'Opinion 03/20 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'. In the document, the WP29 underlines that 'the growing number of situations in which activities of the private sector and of the law enforcement sector interact with each other'[32] imposes to restrict the exceptions to the right to privacy to the strictly necessary. In making such statement, the WP29 refers specifically to financial data transfers to law enforcement authorities and criticises the failure of the proposed legal instruments 'to address the legal uncertainty for situations in which data collected for commercial purposes are used for law enforcement purposes.[33]

Sectorial rules such as those implementing the 5thAMLD, the Market in Financial Instruments Directive framework and the PSD2 can impose data collection and sharing practices that clash with GDRP rules and principles.[34] The complex interaction between the coexisting data protection and data sharing legal frameworks is not straightforwardly derivable from the combined reading of the legal provisions. It remains the task of national policy makers to define to what extent data protection rules can be derogated to enable law enforcement processes. And in practice, the way in which the normative goals are balanced between each other determines - and also depends on - the technical design of the data processing tools chosen by the industry.[35]

The 5thAMLD hints at the role of the Financial Action Task Force (FAFT) in delivering international standards for AML compliance.[36] However, while regulatory frameworks and supranational bodies might give guidance, data-transfer protocols and AML software are mostly developed at a firm or industry level. As it concerns interbank and international data-sharing, a central role is covered by the Society for WorldWide Interbank Financial Telecommunication (SWIFT), which acts as a world leader in the provision of internationally standardised financial messaging services. The cooperative private entity does not only provide software but also acts as Registration Authority for digital identifiers (such as the ISO 9362 Business Identifier Code (BIC) and the

30 Art 16(3)(b) LED.

31 Deloitte, 'After the dust settles - How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on' (2018) <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf> last accessed June 2020.

32 See also: Art 29 Data Protection Working Party (WP29), 'Opinion On Some Key Issues Of The Law Enforcement Directive' <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178> last accessed 10 June 2020.

33 WP29, Opinion 03/2015.

34 See: The Dutch Banking Association, 'The case for further reform of the EU's AML framework' (2019) <https://www.nvb.nl/media/3002/dutch-banking-association_the-case-for-further-reform-of-the-eus-aml-framework.pdf> last accessed 10 June 2020. The report stresses that 'financial market participants need further legal clarity around the interactions between AML and personal data legislation'; Bernadine Reese, 'GDPR and EU AML Directives – A Regulatory Tug-of-War?' (2018) Proviti <https://blog.protiviti.com/2018/05/24/gdpr-eu-aml-directives-regulatory-tug-war/> last accessed 10 June 2020; Bruce Bennett et all, 'Overlap Between the GDPR and PSD2' (2018) Inside Privacy <https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/> last accessed 10 June 2002.

35 Frasher, Agnew (n 3).

36 Recital 4 AMLD.

ISO 13616 International Bank Account Number (IBAN) and ISO 10383 Market Identifier Code (MIC)).

The growing availability of financial data, and the multiplicity of actors that participate in and inform its data processing and exchange processes, demand to scrutinise financial information networks in light of the European data protection legal frameworks. The next paragraph will expose current trends of the financial industry that are making this task more problematic, threatening to make the financial industry a weak spot in EU privacy protection.

III. Financial Information Networks: Weak Spot in European Privacy Protection?

1. The Financial Industry (Changing) Landscape: Digitalisation and Data Economy

Allowing more or less oversight of information by interested actors, the technological infrastructures and the concrete operations in which personal data is involved determine the degree to which privacy policies are enforced. Our analysis seeks to picture how the compromise between privacy and law enforcement is framed in practice. Understanding this practice requires assessing who the information agents involved in data exchanges are; what kind of information do they gather and for which purposes; which roles do these agents perform, under which terms and legal obligations do they collect, use and share information; with which other actors do they share such information.

In the past decades, two major tendencies have emerged that urge to bring the issue of financial privacy in the spotlight. The first one is the digitization of money and commerce, which have exponentially expanded the production and availability of financial data. In 2019, countries like Sweden and the Netherlands have registered a higher total amount of digital transactions than cash-based ones, showing a tendency towards substituting cash even in small-size payments.[37] This trend is interrelated with a wave of 'technology-enabled innovation in financial services' that results in 'new business models, applications, processes or products with an associated material effect on the provision of financial services'.[38]

The second, consequential tendency is the reconfiguration of the incentives underlying the provision of financial services around data exploitation.[39] New tools for data collection and processing and possibilities of intersecting financial data with additional information about users' online activities situate financial information networks within the logics of the contemporary information economy. Arguably, technology has changed practices and modalities of money circulation, and therefore it has reshaped our expectations regarding information management. New actors such as electronic payment providers (PayPal, AliPay) and plastic card issuers (MasterCard, Visa) acquire world-wide dominant position largely due to the optimisation of services that data aggregation allows.

The landscape of financial service providers that intermediate transactions, allocate credit and store value via electronic networks is composite and dynamic. Banking institutions constitute the backbone of global financial flows. Moreover, ancillary yet heavily influential service industries have developed and expanded in word-wide markets. These are, mainly, credit and debit card providers and, more recently, electronic payment providers (e.g. PayPal, AliPay). Finally, a wide variety of non-financial actors process financial data in the context of their commercial activities: retail sellers in physical shops; online e-commerce platforms; credit reporting agencies; insurance companies; marketing agencies, etc.

It is beyond the scope of this paper to focus on specific financial intermediaries or to define the differences in their functions and data practices. We

37 Daphne van Paassen, 'Het is bijna gedaan met de briefjes en munten (maar nog niet helemaal)', De Volkskrant, February 2020 <https://www.volkskrant.nl/nieuws-achtergrond/het-is-bijna-gedaan-met-de-briefjes-en-munten-maar-nog-niet-helemaal~bc49ebab/?referer=https%3A%2F%2Fwww.google.com%2F> last accessed 10 June 2020.

38 Financial Stability Board, 'Monitoring of FinTech' (2017). Examples of such innovative applications are various account aggregation tools such as 'open banking' and 'screen scraping', or roboadvice services; see: OECD, 'Personal Data Use in Financial Services and the Role of Financial Education: A Consumer Centric Analysis' (2020) www.oecd.org/daf/fin/financial-education/Personal-Data-Use-in-Financial-Services-andthe-Role-of-Financial-Education.pdf> last accessed 14th October 2020.

39 Eurpean Banking Federation, 'Data usage, access & sharing in the digital economy' (2020) <https://www.ebf.eu/wp-content/uploads/2020/02/Data-economy-EBF-position-paper-Jan-2020.pdf> last accessed 10 June 2002; World Economic Forum, 'The Appropriate Use of Customer Data in Financial Services' (2018) <http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf> last accessed 10 June 2002.

want, instead, to offer a picture of what the ongoing transition from physical to digital means of payment implies in terms of privacy. Along with electronic payment, mobile banking businesses are examples of 'FinTechs that challenge the traditional financial service sector', as they successfully provide services which 'adjust retail banking to the modern, mobile lifestyle of today's customers'.[40] The terms mobile banking, mobile payments, and mobile transfers refer to various kinds of applications developed to enable storage and transfer of money electronically, via mobile devices such as smartphones and tablets. This type of applications can be developed by existing banking institutions or provided by firms - such as bunq, Revolut and N26 - that centre their business models and products solely around mobile services. As these entities are modelled according to the logics of the data economy, their practices in terms of personal data are considered in the next sections to discuss privacy issues deriving from the latest technological developments of the financial industry.

2. Privacy Loopholes in Financial Intermediaries' Data Practices

a. The Dual Use of Financial Data

The processing of personal data for commercial purposes falls under the scope of application of the GDPR, which limits such processing in order to protect the fundamental rights of data subjects. However, Article 23 GDPR establishes that overriding legal obligations can justify restrictions of such rights. The rights to data portability[41] and data erasure[42], for example, are not granted with regard to data collected in the context of AML procedures. Other examples are Member States' national laws establishing commercial and tax retention periods. For instance, under the German Commercial Code (Handelsgesetzbuch), Tax Code (Abgabenordnung), Banking Act (Kreditwesengesetz), Money-laundering Act (Geldwäschegesetz) and Security Trading Act (Wertpapierhandelsgesetz), the German mobile bank N26 must detain customers' data for a period of two to ten years.[43]

Limitations to the applicability of privacy rules are relevant in light of recent development of the financial service industry towards evermore data-intensive business models. New mobile banking service providers raise particular concerns about the practices of data collection and surveillance that they facilitate.[44] For example, Revolut's privacy statement reveals that the company exploits a wide variety of information for marketing purposes, including the personal information provided by the user to initiate the service, information acquired from social media platforms ('if you allow us to, we will collect information such as friends lists from Facebook or similar information from other online accounts'), information from the user's' device ('contact information from your address book, log-in information, photos, videos or other digital content, check-ins) and information about user's location. Such personal data is shared by default with credit agencies, social media companies, and analytics firms. [45]

The German mobile banking service provider N26 announces in its privacy policy its use of 'Social Plugins': clicking on Facebook, Twitter, LinkedIn or Instagram plugin buttons, users establish a connection between the N26's application and the social media's servers. The social media receives information about the user's visit on the banking app. Regarding this data transmission, the N26's privacy policy remains vague, merely stating that 'as provider of the pages, we do not receive any information on the contents of the data transmitted and their use by Facebook/Twitter/LinkedIn/Instagram'[46]. Moreover, data is shared with third parties in order 'to display specific ads to our customers or to exclude them from specific campaigns'. In particular, using Facebook, Google and Zeotap Custom Audience services, the bank transmits users' email addresses to social media platforms in order to enable the matching of users' profiles with the data possessed by such third parties. No clarification is given about the use that these third parties will make of the shared data.

40 Private Equity Forum, 'Brief insights from PEF research. N26: the rise of a fintech'(2018) <https://pef-jlu.de/wp-content/uploads/2018/10/heyden_poppelreuter_2018_brief_insights_n26.pdf> last accessed 10 June 2020.

41 Art 20 GDPR.

42 Art 17 GDPR.

43 N26 Privacy Policy <https://docs.n26.com/legal/06+EU/03+Privacy%20Policy/en/01privacy-policy-en.pdf> last accessed 12 June 2020.

44 see: Aaron Martin, Mobile Money Platform Surveillance (2019) *Surveillance and Society* <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12924> last accessed 12 June 2020.

45 Revolut Privacy Policy <https://www.revolut.com/legal/privacy> last accessed 12th June 2020.

46 N26 (n 42).

In theory, the principle of purpose limitation prohibits that data collected for law enforcement purposes is used for commercial ones, and vice versa. However, in the case of financial intermediaries, reasons of legal compliance and private commercial interests can overlap. Granular and systemic collection of personal data, in fact, is mandated by sectorial regulation (i.e. MiFID II, 5thAMLD, Transparency Directive, PSD2, national fiscal laws, etc.) aimed at ensuring that transparency, risk management and fraud detection processes are in place. This triggers the exceptional regime allowed by Article 23 GDPR. Yet, the material implementation of security and risk management prescriptions also respond to efficiency considerations that inform the logics of firms' economic strategies.

It is historically accepted that financial intermediaries are custodians of sensitive information: this allows them to support both administrative/judicial processes on one side, and citizens' interaction with the larger economy on the other. Such position, however, becomes critical whereas financial entities expand their data extraction processes to non-financial aspects of private life, intersecting economic information with data points collected by social media or users' devices. Financial firms' data collection strategies must, in fact, be scrutinised considering both the economic interests that incentivise them, and the important decision-making processes they inform in the field of taxation, insurance, credit allocation and judicial investigations.

Finally, the purpose limitation principle is hard to implement because of the fluid nature of enforcement processes. In fact, data previously collected for commercial purposes can then become useful in the context of criminal investigations or required for financial intelligence operations. In such cases, users can have their privacy legal protections diminished without being informed about it.

b. Foreign Access to Financial Data

An interrelated aspect that affects the enforcement of European privacy policies is the cross-national nature of financial services and of the law enforcement networks that are tied to the related data flows. Regulating cross-border data-flows' is particularly tricky when financial data are concerned. On one side, while they expand their businesses across jurisdictions, financial service providers have interest in managing global customers data in a centralised manner.[47] On the other, the governance of their databases is affected by multiple national legal frameworks, as they cover important roles as information agents for national and international law enforcement agencies.

Financial intermediaries move data across countries for a variety of reasons. Often, transaction data is cross-border by nature. Moreover, gathering information in centralised places enables better analytics for risk management and the tailoring of products at regional and local levels.[48] Such movement of data across borders is not, however, uncontroversial from a law enforcement and data protection point of view. In fact, data protection rules established for firms and public authorities in the EU do not always have equivalents in other jurisdictions.

Differences among the EU and the US privacy traditions have, in the past few decades, raised controversies about data sharing practices between law enforcement authorities and financial institutions in the two jurisdictions. Critical differences pertain, for instance, to data retention periods (up to 80 years for US companies, not more than 7 years under the 5thAMLD)[49] and limitations on the commercial use of data (in the EU, firms are bound by the principle of purpose limitation, while in the US the commercial use of data collected for enforcement purposes is not prohibited).

Under the Bank Secrecy Act[50] and the Patriot Act,[51] the US government enjoys wide-ranging powers to obtain data from financial intermediaries, and the latter are unlikely to deny requests of data access from federal authorities. This is a matter of concern as US-based financial firms have ramifications all over the word. The impact of these differences in terms of privacy, surveillance and geopolitical power imbalances becomes glaring if one considers the global pervasiveness of the US financial service industry. While traditional banking is still mainly dominated by local actors, the credit and debit card industry is monopolized by US-based companies (Mas-

47 Selmier, Frasher (n 11).

48 ibid

49 Recital 21 AMLD.

50 The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.).

51 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 200.

tercard[52] and Visa[53]) that make transactions data available to US government and enforcement agencies (e.g. under the Patriot Act). The same can be said about the remittances industry (Western Union, Moneygram and Euronet) and, importantly, the electronic payment service industry (with PayPal in the front line).[54]

'Since banks and other financial services conduct business in many nations but their servers store information from clients around the globe, the location of the server can mean that a European citizen's personal data housed or backed up in New York could be ripe for a subpoena from the U.S. government.'[55]

The reach of the US intelligence over European financial data became a matter of concern when, in 2006, the New York Times revealed the Treasury's Terrorist Finance Tracking Program (TFTP), secretly approved by the Bush Administration to pull EU citizens' data from SWIFT. It was disclosed that the U.S. had secretly subpoenaed the Belgian company SWIFT to hand over information about individuals suspected to be tied to the 9/11 attack. As the servers of the word-wide financial telecommunication network were located in the US, the company handed the personal data of EU citizens to US authorities without applying the legal protections established by EU law.

After the controversy, the company moved its servers to the EU, and – notwithstanding initial pullbacks from the part of the European Parliament[56] - a new agreement between EU and US authorities was concluded in 2010 (SWIFT II).[57] Today, however, concerns about the SWIFT Agreement still exist. The Snowden's revelations demonstrated that 'the US National Security Agency (NSA) has had direct access to the IT systems of a number of private companies and gained direct access to financial payment messages referring to financial transfers and related data'[58] covered by the agreement. In 2013, based on alleged violations of data protection principles of purpose limitation, necessity and proportionality, the European Parliament voted for a suspension of the Agreement,[59] but the Commission has failed to follow-up on such decision.

c. Profiling and automated decision-making

The high volume of data processing performed by financial intermediaries involves the deployment of automated or semi-automated systems for data collection and analysis and algorithm-based consumers profiling.[60] N26, for example, uses semi-automated data processing 'to assess certain personal aspects (profiling)' for the purposes of AML and crime prevention, targeted marketing, and credit risk scoring. Such automated evaluation mechanisms involve the elaboration and matching of a wide variety of personal data including salary, expenses, existing obligations, job, duration of employment, experiences with former contractual relations and credit solvency, 'as well as credit agencies' information'.[61]

The 5thAMLD does not refer to the use of automated or semi-automated mechanisms. However, it mandates 'consumer due diligence', which comprises 'ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship'.[62] Moreover, obliged firms must send Suspicious Transac-

52 Mastercard 'Global Privacy Notice' states that the company shares customers' personal information with Mastercard's headquarters in the U.S and to 'other countries which may not have the same data protection laws as the country in which [the user] initially provided the information' <https://www.mastercard.us/en-us/vision/corp-responsibility/commitment-to-privacy/privacy.html#dataTransfer> last accessed 10 June 2020.

53 Visa Global Privacy Notice states that: 'Visa is based in the United States and has Affiliates and service providers around the world. Your personal information may be transferred to other countries, which may not have similar privacy or data protection laws' <https://www.visa.co.uk/legal/global-privacy-notice.html> last accessed 10 June 2020.

54 PayPal User Corporate rules state that 'Most User Personal Data is collected and stored in the United States. PayPal's global business requires User Personal Data to be shared with other PayPal entities in the United States and globally where PayPal currently has or intends to have a presence.'

55 Frasher, Agnew (n 3).

56 Toby Vogel, 'EU, US sign SWIFT agreement - MEPs' demands for changes accepted', (*Politico*, 28 June 2010) <https://www.politico.eu/article/eu-us-sign-swift-agreement/>last accessed 12 June 2020. For an overview of the controversy about the SWIFT agreement and the TFTP, see: Cristina Blasi Casagran, *Global data protection in the field of law enforcement: An EU perspective* (Routledge 2016).

57 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program.

58 European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)).

59 ibid

60 OECD (n 38)

61 N26 (n 42).

62 Art 13 AMLD.

tions Reporting (STR) to competent Financial Intelligence Units (FIUs). As acknowledged by Europol in its 2017 report on European financial intelligence:

'the increasing digitalisation of financial services results in growing volumes of transactions and extremely large data sets requiring computational analysis to reveal patterns, trends, and associations. The use of analytics is therefore becoming essential for both reporting entities and FIUs to cope with information and fully exploit its potential'.[63]

Customer due diligence and STR are performed through software - made available by technology companies - that uses machine learning for the automated processing of data for customer profiling, transaction monitoring and red flagging. Their output can trigger - based on behavioural patterns and data association - a criminal investigation or denial of a financial product.[64]

Profiling[65] and automated decision-making[66] in the context of AML procedures are legitimate under Article 6(1c) of the GDPR, which establishes a legal basis for automated data processing that is 'necessary for compliance with a legal obligation'. Article 22 GDPR sets out a general prohibition for 'solely automated individual decision', including profiling, which might have a 'legal effect' or be 'significantly affecting' for the data subject. A decision based solely on automated processing, including profiling, however, can be allowed when it is (i) necessary for entering or performing a contract; (ii) authorised by law; or (iii) based on consent.[67] Recital 71 specifies that decision-making based on automated processing, including profiling, shall be allowed when foreseen by national law for fraud and tax-evasion monitoring and prevention purposes, and 'to ensure the security and reliability of a service provided by the controller'.

The WP29 has underlined how profiling and automated decision-making, even when deployed in the context of law enforcement activities, must respect data protection principles and be grounded on a legal basis specified by national law.[68] Data subjects should be granted the right to obtain human intervention from the part of the controller and to 'express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision'.[69] It is questionable, however, whether such rights are granted in the context of automated AML procedures carried out by financial firms. In fact, customers are not informed when reporting is made to FIUs or when a profile has been red flagged. Moreover, algorithm-based transaction monitoring and law enforcement can lead to unfair implementation of compliance procedures. Red flagging and investigation procedures can be triggered by biased automated mechanisms, based on systematic discrimination and stereotyping mechanisms.

Automated data processing and profiling are heavily deployed for credit rating and personalised marketing based on consent. In the opinion of WP29, however, profiling and automated decision-making can involve opaque processes, based on data 'that is derived or inferred from other data, rather than data directly provided by the data subject'.[70] Hence, if these practices are justified based on consent, data controllers must ensure that data subjects are properly informed about the consequences of data processing, and safeguards must be in place to ensure 'fairness, non-discrimination and accuracy in the profiling process'.[71]

Recital 47 concedes that 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'. However, the WP29 reiterates its precedent opinion that 'it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering'.[72] Moreover, the standards for meeting the legitimate interest requirement should be higher in consideration of the com-

63 Financial Intelligence Group, 'From Suspicion to Action, Converting financial intelligence into greater operational impact' (2017).

64 See, for instance: Accenture Consulting, ' evolving AML journey - Operational transformation of anti-money laundering through robotic process automation' <https://www.accenture.com/_acnmedia/PDF-61/Accenture-Operational-Transformation-Anti-Money-Laundering-Robotic-Process-Automation.pdf> last accessed June 2020.

65 Defined by art 4(4) GDPR.

66 Making decisions by technological means without human involvement.

67 Art 22(2)(a)(b)(c) GDPR.

68 WP29, 'Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679'.

69 Recital 38 LED; Art 22 GDPR.

70 WP29 (n 66).

71 ibid

72 WP29 (n 85) recalling WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under art 7 of Directive 95/46/EC (2014).

prehensiveness of the profile and of the relevant impact of such profiling. Credit reporting and scoring, in fact, can significantly impact life opportunities of individuals, determining their likelihood of receiving loans or being offered one rather than another financial product.

On the impact of automated surveillance systems on privacy and liberties, a landmark decision has recently been issued by the Court of The Hague. In the ruling, the Dutch SyRI Act – regulating the use of Systeem Risico Indicatie, an automated system for detecting various kinds of welfare fraud – has been found in violation of Art. 8 of the European Convention on Human Rights. The ruling sets an important precedent in limiting the use of predictive and automated detection systems for law enforcement that contravene fundamental human rights. The Court stressed that Member States must strike 'the right balance between the benefits associated with the use of those technologies on the one hand and the interference that can make use of the right to respect for private life on the other'.[73]

IV. Legal and Technical Steps Toward Financial Privacy

The trends analysed in this paper demonstrate that financial information networks provide opportunities for efficient, capillary surveillance, responding to the interests of both public institutions and private commercial actors. The intensive data collection and analysis demanded by various sectorial legal frameworks compromise some of the legal protections established by the GDPR. While the applicability of privacy rules over financial actors is nuanced due to their quasi-public roles in compliance processes, the financial industry leans toward the logics of a 'surveillance capitalism', with practices of data exploitations that are opaque for both citizens and public authorities.

From a regulatory point of view, the principle of purpose limitations seems to fall short when financial information is concerned. In fact, sensitive information collected in the context of AML, transparency and fraud prevention compliance schemes - interlinked with further information about a person's purchases, geographical movements, social interactions and social media activity - produce datasets that have great economic utility for private and public agencies involved in wealth management. In the regulation of the financial industry, public administration and private economic goals seem to crosshatch in a risk management apparatus built upon information gathering and elaboration. As sectorial rules seek to enhance the role of financial intermediaries as "information brokers", granular and persistent data collection can, therefore, take place at lower data protection standard compared to typical commercial data processing.

Privacy threats also arise from the international nature of financial surveillance networks. As demonstrated by the SWIFT controversies, the liaison between financial intermediaries and public law enforcement agencies can determine intrusions into citizens' financial records from the part of foreign governments. This eventuality is ever more worrisome as the range of data gathered by financial intermediaries expands beyond mere transactional and identification data. For this reason, legal clarification is necessary on how international financial firms handle data of European citizens, and what level of transparency are they demanded from the foreign government and intelligence agencies they respond to. The SWIFT agreement on the matter has showed its shortages in guaranteeing appropriate safeguards against systematic surveillance from the part of US authorities over European citizens. As the Privacy Shield is not applicable to the exchange of financial data, clearer conditions for transnational data transfers should be established.

The capillarity and ubiquity of financial surveillance and enforcement networks can be challenged under multiple legal considerations. Forms of data-driven automated enforcement threatens privacy, individual autonomy, fairness and democratic values.[74] The argument in favour of financial anonymity gains strength in view of the possible risks that 'perfect' surveillance and enforcement - in the form of full traceability and record-keeping - entail in terms of fundamental rights. This is not only true when informational power is abused by profit-driven private intermediaries or totalitarian political powers. Risk-based, pre-emptive law enforcement systems based on surveillance and social sorting undermine key

73 *NJCM et al. and FNV v The State Of The Netherlands* [2020], ECLI:NL:RBDHA:2020:865.

74 Yeung (n 18)

principles of due process and can have subtle biased outcomes even when deployed for the purpose of 'efficient' administration.[75]

Spaces for confidential financial transactions - which are progressively eroded with the ongoing disappearance of cash - are necessary to counteract the risks of absolute surveillance. The European Central bank recognises the need for anonymous payment methods in a report of December 2019, where it establishes a proof of concept for an anonymous 'central bank digital currency' (CBDC).[76] Even more, the necessity for anonymous online means of payment has emerged vigorously from privacy-aware online communities which - in the past two decades - have developed open-source software solutions for transacting under pseudonymous accounts. Prominent efforts toward financial privacy are made by developers of peer-to-peer, digitally-native currencies based on permissionless blockchains (e.g. bitcoin, ethereum, Dash, Zcash, Monero, etc.). In the meantime, technological firms are working on the development of privacy-preserving technology for online payments connected to state-backed currency (e.g. GNU Taler[77]).

As the possibility to transact anonymously is not prevented by the legal frameworks on anti-money laundering and counter-terrorist financing when payments under a certain amount are concerned, policy-makers should take over the task of enabling the normative goal of financial privacy at the technical level as well. By promoting and facilitating initiatives that seek to build systems for confidential financial applications, governments would not only respond to citizens' legitimate interests; they would also put themselves in the position to ensure that such applications develop within a clear legal and institutional framework. If, on the contrary, public authorities will keep contrasting the development of anonymous/pseudonymous means of digital payment, bottom-up solutions will continue to emerge, responding to the need of financial confidentiality in manners that might be more extreme, less detectable, less understandable to law enforcement and monetary institutions. They would, likely, exacerbate the very same risks that AML/KYC policies are meant to eradicate, while bringing the option of financial anonymity only at the disposal of narrowly defined, possibly ill-intentioned societal groups.

By contributing to the construction of a technical infrastructure for confidential digital payments, institutions could promote solutions that incorporate both privacy and law enforcement legal requirements. Establishing a compromise between private commercial interests, public quest for transparency and law enforcement requirements, top-down and bottom-up initiatives can be integrated to respond to the priorities of diverse interest groups, putting citizens' fundamental rights first.

V. Conclusions

The present article illustrates how, in the governance and regulation of financial data, privacy considerations are compromised with law enforcement priorities. Knowledge about people's financial status is necessary for the administration of modern societies and for the protection of public interests. Tracking financial records facilitates the efficient allocation of resources and the administration of welfare and criminal policies. As these legitimate interests inform the management of financial data, the operability of GDPR legal protections is partially compromised.

The GDPR, in fact, allows exceptions to privacy protection when law enforcement legal obligations are imposed - e.g. by AML legal rules - on information intermediaries. However, the wordings of the LED, of the GDPR and of the 5thAMLD, as well as the opinion expressed by WP29, indicate that law enforcement policies must respect the principles of data protection (i.e. data minimisation; purpose limitation) and be limited to what is strictly necessary, respecting fundamental individual rights.

Compromising privacy in the name of law enforcement can be a slippery slope. The reasons justifying data collection and processing from the part of financial institutions are not always univocal: the very same pieces of data and their triangulation can serve multiple purposes. Notwithstanding the semi-public roles that financial intermediaries are ascribed based on their role as information agents, such entities are commercial entities incentivised by profit maximisation goals. Data gives financial firms competitive

75 Yeung (n 18).

76 European Central Bank, 'Exploring anonymity in central bank digital currencies', Issue n.4, December 2019.

77 Jeffrey Burdges et al, 'Enabling Secure Web Payments with GNU Taler' (2016) <https://taler.net/papers/taler2016space.pdf> last accessed 12 June 2020.

advantage over other financial firms, it allows to target products and services at a regional and at an individual level, and it can be exchanged with third parties for credit risk profiling. Processed in automated manners for profiling and marketing purposes, financial data are not immune from practices of accumulation for profit maximization and re-engineering of behaviours through algorithm-based predictive technologies.

Exposing financial entities' practices of data commercial exploitation, and issues related to the transfer of those data to third parties - including foreign law enforcement agencies and social media platforms - the study argues that financial data constitutes a weak spot of European privacy protection. The analysis provided in the present work suggests that legal clarification is necessary a) about the implementation of the purpose limitation principle, to ensure that financial data collected for law enforcement purposes is not abused in commercial data-intensive strategies; b) on the jurisdictional limitations of law enforcement data-access; and c) on the use of automated decision-making and profiling from the part of financial institutions, in the context of their compliance processes, credit risk scoring and marketing strategies.

As physical cash is replaced by digital means of payments even for small-size transactions, financial data becomes increasingly available, informative and interlinkable to various personal information. The capillarity and ubiquity of financial surveillance performed thought automated data processing is questionable from a privacy point of view; it limits individual freedom and autonomy and threatens fairness and indiscrimination in administrative and criminal procedures. Based on the view that the coexistence of privacy and law enforcement goals requires to admit spaces where one or the other goal is sacrificed for the benefit of the other, this paper argues for the necessity and legitimacy of tools for anonymous (or pseudonymous) digital payments.

To counteract the risks of a financial industry that buys into the logics 'surveillance capitalism' on one side, and the threats of uncontrolled anonymous money technologies on the other, public institutions should play a role in the development of privacy-enhancing payment methods. To this aim, research efforts and political commitment are needed for the development of confidential online payment solutions, which can be set to work within the boundaries of overriding security and law enforcement limitations.[78]

78 The author of this paper is in the process of writing a follow-up paper on the techno-institutional conditions and legal implications of anonymous digital payment methods.