Public-Private Financial Information-Sharing Partnerships in the Fight Against Terrorism Financing:

Mapping the Legal and Ethical Stakes

Maja Dehouck
Marieke de Goede

University of Amsterdam
January 2021

University of Amsterdam

Project craaft
Collaboration, Research & Analysis Against the Financing of Terrorism

Public-Private Financial Information-Sharing Partnerships in the Fight Against Terrorism Financing: Mapping the Legal and Ethical Stakes

Published on 5 January 2021 by the University of Amsterdam

Authors: Maja Dehouck and Marieke de Goede

This publication is published in open access format and distributed under the terms of the Creative Commons Attribution-Non-Commercial-No-Derivatives License, which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited and is not altered, transformed, or built upon in any way.

The views and recommendations expressed in this publication are those of the authors and do not reflect the views of UvA or any other institution.

University of Amsterdam

Project craaft
Collaboration, Research & Analysis Against the Financing of Terrorism

This project was funded by the European Union's Internal Security Fund – Police

About

This report is part of a three-year research project on the ethical and legal challenges of public-private financial information sharing at the University of Amsterdam, as part of Project CRAAFT.

Project CRAAFT (Collaboration, Research & Analysis Against the Financing of Terrorism) is an academic research and community-building project designed to build stronger, more coordinated counter-terrorism financing (CFT) capacity across the EU and in its neighbourhooda.The project engages with authorities and private entities in order to promote cross-border connectivity and targeted research.

Funded by the European Union's Internal Security Fund – Police, the project is being implemented by a Consortium led by RUSI Europe, along with the University of Amsterdam, Bratislava-based think tank GLOBSEC and the International Centre for Counter-Terrorism (ICCT), based in The Hague. For more information, see: https://www.projectcraaft.eu/

About the authors

Maja Dehouck is a researcher at the Department of Political Science at the University of Amsterdam. She holds an LLM in International and European Law from Tilburg University and an MSc in Social and Cultural Anthropology from KU Leuven. Her areas of research include counter-terrorism financing and the illicit trade in cultural goods.

Marieke de Goede is Professor of Political Science at the University of Amsterdam with nearly 20 years of experience in research on counter-terrorism financing. She is author of *Speculative Security: the Politics of Pursuing Terrorist Monies* (University of Minnesota Press) and is Principal Investigator of *Project FOLLOW: Following the Money from Transaction to Trial* (www.projectfollow.org). She has published a report (in Dutch) with Mara Wesseling on *Counter Terrorism Financing Policies in The Netherlands: Effectiveness and Effects* (2018), via: https://repository.tudelft.nl/view/wodc/uuid%3Abf9e1d87-fbb6-41ff-a1a6-f0d477d32b78

Acknowledgements

Many thanks to the members of Project CRAAFT and Project FOLLOW for their constructive feedback on an earlier version of this report. In particular, we would like to thank Tasniem Anwar, Andreas Baur, Rocco Bellanova, Esmé Bosma, Tom Keatinge, Pieter Lagerwaard, Anneroos Planqué-van Hardeveld, Kinga Redlowska, Stephen Reimer and Carola Westermeier. Special thanks to the two anonymous reviewers and to Philippe de Koster and Hans Van Hemelrijck for their input.

This research received funding from the EU Internal Security Fund [grant agreement No. 878484 - CRAAFT]. Additionally, this project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme [grant agreement No. 682317].

Contents

SUMMARY 05

INTRODUCTION 06

PART A. BACKGROUND: FISPs AND FINANCIAL SURVEILLANCE 07
Financial Information-Sharing Partnerships 08
Relevance of the research 09
Approach 10

PART B. LEGAL AND ETHICAL DIMENSIONS 12
I. Democratic legitimacy 13
Establishment process 13
Legal basis 13
Necessity 14
Composition 14
Legitimate aim 14

II. Privacy and proportionality 17
Scope 17
Nature of the information exchanged 17
Access to information 18
Data protection 18
Profiling 19

III. Mistakes and misuse 22
Mistakes 22
Unintentional misuse 22
Intentional misuse 23

IV. Rights of individuals 25
Redress 25
De-risking 25

V. Accountability 27
Internal accountability 27
Oversight 27
Transparency 27
Sanctions 28

CONCLUSION 30

Annex 1: Key questions overview 31

Annex 2: Sources cited 34

SUMMARY

Financial Information-Sharing Partnerships (FISPs) have emerged in the context of broad trends in global Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) regulation. What is unique to FISPs is that they enable law enforcement information, including personal data, to be proactively shared with private industry actors. They constitute a cornerstone of future CFT efforts.

The legal and ethical challenges of FISPs remain insufficiently understood. These challenges include good governance, transparency and the protection of the rights of citizens whose data are shared. This report maps the ethical and legal dimensions of FISPs, as a first step in a broader study on legal embedding and ethical practices of financial information sharing.

This report distinguishes five clusters of legal-ethical challenges and formulates relevant questions to be asked by and of FISPs for each area.

I. Democratic legitimacy

The democratic legitimacy of a FISP hinges on both the democratic process through which the partnership was established, and the foundations of the partnership which have been laid down through that process. These foundations consist of the necessity for the partnership, its legal basis, its composition, and the boundaries of its purpose.

II. Privacy and proportionality

Consistency with the principle of proportionality is crucial for FISPs[1]. In order to ensure this, it is imperative to identify any limits to the exercise of democratic rights and civil liberties. Perhaps the most pressing concern in that regard is compatibility with privacy standards and law.[2] This compatibility can be gauged along the lines of the scope and nature of the information exchanged, access to information, data protection and profiling.

III. Mistakes and misuse

FISPs hold a risk of producing adverse impacts when they are not used for the purpose or in the ways in which they were intended, or when their set-up is inherently flawed. What exactly constitutes misuse within any given FISP depends on how the aims, the legal obligations and ethical conduct have been defined. Misuse can manifest in many different ways and can be intentional or unintentional.

IV. Rights of individuals

Another cluster of challenges identified in this report is the rights of individuals who have been identified as part of a FISP investigation. We outline two sets of questions which may assess whether persons identified within a FISP can find appropriate remedy and are sufficiently protected against de-risking.

V. Accountability

Ensuring accountability is important in a context where sensitive law enforcement information is passed between public and private spheres. Oversight and accountability can help address some of the potential harms of profiling, mistakes and misuse outlined in previous clusters. This report outlines four aspects of accountability, namely internal accountability, oversight, transparency and sanctions.

A full overview of the key questions identified throughout the report can be found in annex 1.

1 de Oliveira, 2016
2 Reidenberg, 2001

INTRODUCTION

Since 2015, new forms of public-private partnerships for financial information sharing have been established around the world, with the aim of countering terrorism financing and financial crime[3].

FISPs form a new platform in the combat against terrorism financing, as they allow law enforcement information, including personal data, to be proactively shared with private industry actors. Financial information-sharing partnerships are said to mark a fundamental shift towards closer public-private collaboration and a more targeted approach to combating terrorism financing efforts.[4][5]

However, a number of crucial questions around the legal and ethical dimensions of FISPs remain insufficiently understood by stakeholders, practitioners and academia[6]. These include for example issues around good governance, transparency and the protection of the rights of citizens whose data is shared. The premise of this report is that ethical and legal concerns regarding financial intelligence in general, manifest themselves in specific ways in financial information-sharing partnerships.

This report maps the legal and ethical dimensions of FISPs, anchored in the academic literature on privacy, proportionality and surveillance ethics. The objective of the report is threefold:

- First, to offer a comprehensive overview of the ethical and legal dimensions of FISPs;
- Second, to develop a framework of questions to gauge existing and future partnerships in terms of their legal and ethical challenges;
- Third, to lay down the groundwork for the next research phase, i.e. an analysis of the state of affairs based on fieldwork in four case study countries, in order to provide best practice recommendations.

The report identifies five areas at the intersection of legality and ethics, relating to public-private partnerships for financial information sharing. Within each area, we propose a broad set of questions to be asked by and of FISPs.

FISPs exist within varying national contexts and jurisdictions that shape their construction and practices[7]. Therefore, the aim of this report is to offer a broad framework to gauge any existing or future partnership in terms of its legal and ethical challenges, rather than providing a detailed analysis of certain partnerships in particular.

The next phase of this project will offer an analysis of the state of affairs based on fieldwork in four case study countries, with the aim of providing best practice recommendations. Where necessary, corrective or complementary measures and the improvement of policies and processes can be based on the findings of this research. As such, the present study is intended to contribute to strengthening FISPs democratic legitimacy, ethical integrity and legal basis.

3 Maxwell, 2020
4 Our focus in this report is confined to counter-terrorism financing (CFT) measures, although the discussion can also be applied to the anti-money laundering (AML) regime.
5 Maxwell & Artingstall, 2017: p. x; Europol, 2017; Clearinghouse 2017; Wesseling and de Goede 2018.
6 Maxwell & Artingstall, 2017
7 Maxwell, 2020

PART A.
BACKGROUND: FISPs AND FINANCIAL SURVEILLANCE

FINANCIAL INFORMATION-SHARING PARTNERSHIPS

Financial Information-Sharing Partnerships (FISP) have emerged in the context of broad trends in global Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) regulation. The solidification of FISPs constitutes a cornerstone of future CFT efforts, and the potential to expand them to other types of crime and other types of industry is being explored.[8]

FISPs are a type of Public-Private Partnership (PPP) that involves new collaborations between public institutions (e.g. law enforcement and Financial Intelligence Units) and private partners (e.g. banks, insurance companies, money transfer providers).

The global AML and CFT regulatory context of FISPs is shaped by, *inter alia*, the standards and recommendations of the intergovernmental Financial Action Task Force (FATF), the EU Fourth and Fifth Money Laundering Directives, and UN Security Council Resolutions 1267, 1373 and 2462.[9] These oblige banks, financial institutions, insurance companies and other entities to identify transactions that are abnormal or suspicious in the context of terrorism financing. It is known that only a small number of suspicious transactions reports are associated with terrorism financing – less than 1% of those filed at all Financial Intelligence Units (FIUs) across the EU, according to a 2017 report.[10]

The modus operandi of FISPs can range from sharing knowledge and threat analyses, to exchanging operational information and personal data.[11] What is unique to FISPs is that they allow law enforcement information, including the names of specific individuals or other identifying information, to be *proactively* shared with private industry actors.[12] This reverses the flow of information and renders it more dynamic in the chain of financial transactions monitoring.[13] Most FISPs are based on existing legal frameworks. At the same time, pro-active operational data sharing from law enforcement to private industry operates at the limits of existing legal frameworks.[14]

FISPs generally promise more targeted information sharing and a better cost-benefit balance to industry partners than large-scale transactions monitoring. A recent Europol report praises the potential of FISPs and calls for more *"targeted"* approaches in financial intelligence, whereby *"intelligence feeds from law enforcement agencies [act] as the basis for proactive financial crime investigations."*[15]

The targeted sharing of police information and personal data with private partners through FISPs raises considerable legal and ethical questions. When ideas of this kind were first suggested in the wake of the 9/11 attacks, the 9/11 Commission acknowledged the potential effectiveness of sharing intelligence and law enforcement information with private partners like banks, but also expressed grave concerns: *"Providing intelligence about terrorist financing to bank personnel raises serious privacy and civil liberty issues. (...) Turning [intelligence] reports over to private citizens like bank personnel runs the risk that entirely unsubstantiated allegations may lead banks to shut customer accounts or take other adverse action."*[16] Though the 9/11 Commission here speaks of intelligence information, law enforcement information may suffer similar limitations. This report maps and examines the legal and ethical questions that are applicable to FISPs and financial surveillance more broadly.

8 Maxwell, 2019
9 An overview of all relevant regulation exceeds the scope of this report. See: King, Walker & Gurulé, 2018.
10 Europol, 2017: p. 40
11 Maxwell & Artingstall, 2017
12 Maxwell, 2020
13 de Goede, 2018
14 Wesseling and de Goede 2018.
15 Europol, 2017: p. 40; see also Clearinghouse 2017
16 Roth, Greenberg & Wille, 2019: p. 64

RELEVANCE OF THE RESEARCH

Sound legal and ethical bases are key to the future of FISPs. They will provide existing and future partnerships with the necessary political and democratic legitimacy to operate in alignment with commitments to human rights and civil liberties, and the principles of good governance, legislative clarity and transparency.[17] The ethical and legal dimensions of FISPs have several broad implications which underscore the importance and urgency of research into them.

Financial surveillance in general affects the rights and lives of citizens, and FISPs do so in specific ways. FISP activities affect all clients of the reporting entity whose financial data is being surveilled, all persons whose information has been shared between public and private (or private-private) entities, individuals who have been the subject of an information request by law enforcement to private reporting entities, and persons or demographics who have been the victim of wrongful or excessive surveillance (e.g. as the consequence of bias or misuse).

Financial surveillance risks indirectly generating chilling effects, whereby knowledge of the existence of surveillance activities for counter-terrorism purposes discourages citizens from engaging in legitimate behaviour.[18] Examples include refraining from donating to charities which address important humanitarian needs[19], or from sending remittances. There is no clear view on the chilling effects of public-private partnerships in particular yet, as in-depth studies on this risk are lacking.[20]

Legal embedding and ethical practices within FISPs are of importance to society at large and the values and principles it upholds as its cornerstones, such as democratic accountability and respect for human rights and civil liberties. To the extent to which operations disregard ethical considerations, they risk eroding the human rights records and democracies of the countries where they are in place.

Existing and emerging forms of FISPs create precedents for future partnerships. As pioneers in the field of sharing operational data between public and private institutions, they set general standards for ethical practice and the legal basis for these types of partnerships. The precedent set by FISPs may influence legal and ethical standards of future partnerships, including in countries where the harm to liberties is more acute than in the countries where FISPs originated.[21] When, in these circumstances, new partnerships are modelled after existing ones where legal and ethical questions have not adequately been addressed, the rights of citizens in other countries may be jeopardized.[22] This in turn may harm the credibility and reputation of FISPs in general. It might also complicate diplomatic efforts in promoting human rights abroad and it might erode the credibility of the EU's leading role in setting the global standard for data protection.[23]

Non-financial sectors such as the art market are moving into the AML/CFT-regulated space, which requires them to conduct checks on customers and to detect and report suspicious transactions.[24] There is also increased interest in the intelligence value of social media companies, as terrorists expand beyond banks to new payment systems and funding avenues.[25] The potential for extending models for information-sharing partnerships from the financial sector to other types of reporting entities raises the question of what kind of precedent they set in terms of their ethical and legal legitimacy.

17 Maxwell & Artingstall, 2017: pp. 27-39
18 Swire, 1999
19 Atia, 2007; Chong, 2020; ACLU, 2009
20 Büchi et al., 2020: p. 6
21 Swire, 1999
22 See also Etzioni, 2018
23 Purtova, 2018; Andrew & Baker, 2019
24 Hufnagel & King, 2020
25 Keatinge & Keen, 2020; Davis, 2020

APPROACH

The present report builds on previous research as well as emerging work on FISPs, in order to map the ethical and legal dimensions of FISPs.

FISPs emerged from a CFT financial surveillance regime that rests on three existing pillars: (1) suspicious transactions reporting by banks, money remitters and other reporting entities; (2) listing and designation by national governments and supranational institutions; and (3) juridically regulated law enforcement data requests in the context of law enforcement investigations.

Transactions monitoring is a form of financial surveillance where large databases of the financial transactions of banks, money service businesses and other reporting entities are analysed and mined for abnormal patterns and behaviour. Listing is a practice whereby named individual or entities are placed on one of over 200 national or international watchlists.[26] FISPs are a new form of public-private partnership and financial data sharing that holds ground between monitoring and listing: in such partnerships, data on named individuals and suspects is proactively shared by law enforcement with private industry partners.

A large body of research exists on the challenges and harms caused by listing and suspicious transactions monitoring, and financial surveillance more broadly. As CFT efforts increasingly evolve into a FISP-based system, they are deserving of the same research attention as the previous measures of listing and suspicious transactions monitoring.

Maxwell and Artingstall offer the most comprehensive analysis of FISPs to date, including an overview of their various forms, methods and their legal and political questions.[27] In their 2017 report, Maxwell and Artingstall set out the elements for a *"principles-based approach to information sharing,"* and offer a set of recommendations ranging from robust governance structures to effective oversight and transparency of metrics.[28] This report builds upon this body of work in order to develop a comprehensive mapping of the legal and ethical challenges surrounding FISPs.

The present mapping of the ethical and legal questions relevant to FISPs is embedded in academic literature and international governance frameworks. We take ethical and legal aspects and potential harms together. First, it is important to identify and assess the legal context of FISPs, which is not always clear-cut as FISPs operate at the intersection between security objectives and data protection law. Second, it is important to consider the ethical implications of the types of (personal) information sharing taking place within FISPs. Ethics is broader than legal compliance, and ethical implications of data practices can be contextual. Ethical concerns relating to FISPs include for example good governance, transparency and the protection of the rights of citizens whose data is shared. There are also ethical concerns around regulating the relations between public and private actors, and questions concerning security clearance and liability for private participants in FISPs. In order to map and understand ethical concerns, it is an accepted practice to work with a list of questions that can help professionals reflect on their practices.[29]

This report starts from the Fair Information Practices as initially developed by the US Health, Education, and Welfare Department in the 1970s, which subsequently informed the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[30] In 1998, sociologist Gary T. Marx published an updated version of the Fair Information Practices that takes new technologies and new types of data sharing into account. Marx's template is structured as a set of twenty-nine *"Questions to Help Determine the Ethics of Surveillance,"* subdivided into questions on 'means,' 'context' and 'use.'[31] Marx outlines a set of questions to address ethical challenges of data sharing and data mining.

26 De Goede & Sullivan, 2016.
27 Maxwell & Artingstall, 2017
28 Maxwell & Artingstall, 2017: pp. 27-44.
29 Wright 2010; see also Wright et al., 2015
30 OECD, sd
31 Marx, 1998: p. 174

This report draws upon Marx's framework for the ethics of surveillance and has adapted his twenty-nine questions to the purpose of assessing FISPs and other types of public-private information-sharing partnerships and networks. We distinguish five clusters of legal-ethical challenges, and formulate relevant questions to be asked by and of FISPs for each cluster:

I. Democratic legitimacy
II. Privacy and proportionality
III. Mistakes and misuse
IV. Rights of individuals
V. Accountability

Clusters I and II are designed to ensure that FISPs are founded on a sound ethical and legal basis. They are intended to cover the ground of a solid foundation for FISPs, in order to maximize their legitimacy, legal embedding and ethical practice. Cluster III is concerned with the ways that harms to individuals or groups may still occur in spite of the ethical and legal embedding of FISPs. The last two clusters cover ways to mitigate and remedy those harmful impacts at the individual and partnership levels.

The discussion that follows is broadly framed to address different types of public-private information sharing and different types of data. Not all issues are expected to be equally relevant to all FISPs, as they all have different national legal and ethical contexts that shape their construction and practices.

PART B.
LEGAL AND ETHICAL DIMENSIONS

I. DEMOCRATIC LEGITIMACY

FISP entail close cooperation between public agencies and private companies in the fulfilment of traditionally public functions of crime prevention and investigation. They entail a transfer of power and responsibility[32] which fits in a broader trend whereby policing activities rely on the vigilance of private actors.[33] Sharing responsibility between public agencies and private actors in contributing to the common good[34] requires a solid legal and democratic basis.

The democratic legitimacy of a FISP hinges on both the democratic process through which the partnership was established, and the foundations of the partnership which have been laid down through that process. These foundations consist of the need for the partnership, its legal basis, its composition, and the boundaries of its purpose.

Establishment process

A key component of the democratic legitimacy of a FISP is whether its establishment was arrived at through democratic decision-making procedures; in other words, whether the decisions around setting up the partnership were subject to public discussion and political deliberation prior to its start. The public discussion component entails whether the general public is informed of the purpose of financial information sharing[35] and whether public debate is fostered preceding decisions on the foundations of the partnership, e.g. in the media or other public forums. Political deliberation includes parliamentary debate, stakeholder involvement and civil society consultation. Of importance thereby is whether the parties involved sufficiently represent the interests of all layers of society.[36]

Allowing public insight and participation in the establishment process implies considerable transparency from the very start, which may have to be balanced against the need for a certain degree of secrecy.[37] It must also be noted that public discussion on financial information sharing for CFT purposes can be challenging, as the subject matter is complex and controversial.

Legal basis

The main prerequisite to the establishment of a FISP is to ascertain that there is a sufficient legal basis. Sharing police information and personal data of potential suspects with private actors is strictly regulated. There are good reasons why police information is protected and police suspects have rights in democratic societies. In some cases, FISPs handle personal information of persons who are not yet suspects in the formal sense, but who have come to the attention of police. Therefore, legitimacy in setting up a FISP hinges on whether there is a sufficient legal basis to give private actors the authority to carry out this type of surveillance activities, in the jurisdiction where the FISP is to operate.

Generally, a distinction can be made between FISPs whereby the legal basis is grounded in existing law which was not explicitly drafted with FISPs in mind, and cases whereby a legal basis is created through new legislation drafted with the explicit purpose of creating the FISP. The choice for either system may have implications on the degree of uncertainty around the partnership's legal legitimacy, which may linger after its establishment. As Maxwell and Artingstall note, legislative clarity is crucial to ensure *"private sector confidence in the interpretation of the legal gateway for information sharing."*[38]

32 Ross & Hannan, 2007
33 Amicelle & Favarel-Garrigues, 2012: p. 105
34 Etzioni, 2018: p. 6
35 Diderichsen & Ronn, 2017
36 Wright et al., 2015: p. 291
37 Diderichsen & Ronn, 2017
38 Maxwell & Artingstall, 2017: p. 31.

Necessity

A second preliminary component to be discussed prior to setting up a FISP is its place in the wider AML/CFT regime. The question of necessity in general entails whether alternative, less harmful means to achieve the same end have been explored and deemed insufficient.[39] Applied to FISPs in particular, necessity translates to the question of whether the need for a FISP as an alternative or addition to the existing CFT regime, has been demonstrated. It also means balancing the intrusiveness of the measure with its results.

A myriad of obligations and engagements are in place to counter the financing of terrorism, all with their challenges for fundamental rights, their burdens on financial institutions, and their mixed results.[40] Prior to setting up a FISP, there should be democratic deliberation on the ways the existing regime has proven insufficient or otherwise undesirable, and why the FISP is expected to remedy the deficiencies of the existing system. Part of that question is whether the partnership is intended to supplement the existing regime, or is meant to serve as a replacement of past programmes or current ones which are to be discontinued. Lastly, have alternatives to a FISP been examined to achieve the same goal of remedying the shortcomings of the current CFT regime?

Composition

Once the legal basis and the place of the FISP in the wider CFT regime are established, a third foundation of the FISP which deserves closer scrutiny is its composition. This means: on what basis is decided which parties are included in the partnership? Are partners included based on formal requirements such as their recognition as a financial institution, or rather on informal trust relations? This question bears particular importance to, for instance, tech companies operating in the sphere of new payment systems and cryptocurrencies.

Inclusion in a Financial Information-Sharing Partnership entails access to privacy-sensitive and security information. Consequently, in assembling the partnership the trustworthiness of partners involved is of vital importance. It must also be examined whether the inclusion of certain private sector parties produces a competitive disadvantage towards excluded institutions, or vice versa. For instance, inclusion in a partnership, especially in addition to existing obligations, places additional burdens on the private sector partner which excluded companies do not have. On the other hand, particularly concerning new players on the market, being included in a FISP may provide a certain legitimacy which may translate to reputational advantages over excluded companies.

Legitimate aim

The last of the FISP foundations to be subjected to democratic deliberation is the definition and justification of its objectives; in other words: questions on the purpose of setting up a FISP, what it is intended to do, and what the limits of its purpose are. Democratic control is needed as a means of ensuring that the activities serve legitimate interests[41]. The boundaries to the purpose of information sharing impact *inter alia* issues of function creep, misuse and the kinds of information to be exchanged, which will be detailed further below.

For what concerns surveillance in general, there is no objective standard to determine which objectives are legitimate.[42] States' positive duties to defend and protect their citizens and to uphold the rule of law are generally cited as a justification

39 Macnish, 2014
40 King, Walker & Gurulé, 2018; Wesseling & de Goede, 2018
41 Gould, 2019
42 Omand & Phytian, 2013

for the limitation of certain rights in the fight against terrorism.[43] However, there is a general consensus that the aims of surveillance activities must be specifically justified and well-delineated if one is to avoid them spilling over to unjustified purposes such as bureaucratic empire building or political or personal gain.[44]

Three main issues demonstrate the importance of clear and justified boundaries to the goals of public-private information sharing for CFT purposes: First, the purpose of targeted forms of surveillance in particular requires clear confines, as they carry grave dangers when employed as a tool for the repression of human rights defenders and other unlawfully targeted groups.[45] Secondly, the boundaries of certain CFT measures are contested due to the pre-emptive security logic underlying them.[46] Third, given the blurred lines between private corporations and law enforcement in FISPs, specific attention must be paid to the compatibility of corporate business interests with the public interest,[47] such as the risk of function creep linked to the commercial use of financial intelligence data.

It is therefore important that the goals of any FISP are made explicit, are specific and are justified[48] as part of the democratic process detailed in the previous section. The main question to be deliberated on is how the objectives of the FISP are to be defined and justified. Connected to that is attention for how much flexibility the boundaries of its purpose allow: do they leave much room for interpretation or are they strictly delineated?

43 Omand & Phytian, 2013: p. 52
44 Omand & Phytian, 2013: p. 53
45 Amnesty International, 2019
46 Anwar, 2020: p. 390. See also Opitz & Tellmann, 2014; de Goede, 2014
47 Helgesson, 2011
48 The purpose specification of the collection of personal data to "specific, explicit and legitimate" purposes is also codified in law, for instance in GDPR Article 5.1b.

Key questions
Cluster I: Democratic legitimacy

Establishment process

- Was the FISP established through democratic decision-making procedures?
- Was the decision to set up the partnership subject to public discussion and political deliberation prior to its start?

Legal basis

- What is the legal basis of the FISP?
- Is the legal basis of the FISP grounded in existing law or through enabling legislation drafted with the explicit purpose of creating the FISP?

Necessity

- Has the need for a FISP as an alternative or addition to the existing CFT regime been demonstrated?

Composition

- On what basis are decisions made regarding which institutions to include in the partnership?
- Does the inclusion of certain private sector institutions produce a competitive disadvantage towards excluded institutions, or vice versa?

Legitimate aim

- How are the objectives of the partnership defined and justified?
- To what extent do the boundaries of its purpose allow for flexibility?

II. PRIVACY AND PROPORTIONALITY

Consistency with the principles of privacy and proportionality is crucial for FISPs.[49] In order to ensure this, any limits to the exercise of democratic rights and civil liberties caused by surveillance and data processing must be identified.[50] Perhaps the most pressing concerns in this regard are compatibility with privacy standards and data protection law. This compatibility can be gauged along the lines of the scope, the nature of the information exchanged, access to information, data protection and profiling.

The extensive obligations that financial institutions and reporting entities have under AML/CFT law create tensions with privacy laws and the data protection of client information, especially in the context of the EU General Data Protection Regulation (GDPR).[51] These are part of wider debates on the tension between security and privacy, and the common good versus individual rights.[52] Following the principle of proportionality,[53] the usefulness of financial information for counter-terrorism and other security purposes must be weighed against the limits to privacy.[54]

Scope

A key element to assess proportionality with respect to financial surveillance is its scope, i.e. the number of persons affected. Data protection law and principles stipulate the principle of minimization, i.e. the limitation of data collection to what is strictly necessary for the specified purposes.[55]

In principle, FISP operations are more targeted than large-scale transactions monitoring. Nonetheless, questions of proportionality remain relevant as their modus operandi implies the collection, retention and analysis of large databases of identified individuals. A number of factors may expand the scope of FISP activities. For instance, the use of network analysis exponentially expands the scale of data retained and persons affected.[56] The principle of proportionality requires attention to the limits of the degree of separation to which a connection to (suspected) terrorism financing justifies data collection about a person. Pooling information from other sources is another factor which may expand the scale of affected people. Lastly, an implicit but structural incentive for defensive over-reporting of suspicious activity has been observed in the past.[57] These issues, among others, require the consideration of questions with respect to the number of people affected by information sharing through FISPs and whether the scope of data collection respects the principle of proportionality.

Nature of the information exchanged

A second determinant to assess the proportionality of financial surveillance is the level of intrusiveness. This covers limits as to which type of data is collected and shared. In FISPs, the information shared may be limited to typologies and expertise. But FISPs may also share personal data such as names, addresses, social security numbers, bank account information and other personal details.

Sharing financial and banking information allows precise conclusions to be drawn about the private lives of individuals.[58] When aggregated over time or with other data sources, it can reveal information about sexual orientation, medical history, purchase history and location information.[59]

49 de Oliveira, 2016
50 Roessler, 2017; Lyon, 2014; European Data Protection Supervisor, 2020
51 Frasher, 2013
52 Etzioni, 2018
53 Lyon, 2003; Sharman, 2009
54 Rogovin, 1986
55 Andrew & Baker, 2019; Marx, 1998: p. 178.
56 Wesseling & de Goede, 2018: pp. 227-228.
57 Amicelle & Iafolla, 2018
58 Sharman, 2009
59 Amnesty International, 2017: p. 28

Perhaps even more than communications data, *"Personal bank records provide a 'virtual current biography' of a person's life, revealing not only financial data, but information about opinions, habits and associations as well"*.[60] Although this information constitutes a key intelligence-gathering tool for law enforcement and security services,[61] it also jeopardizes several privacy aspects, such as:

- 'privacy of behaviour and action', e.g. political activities, religious practices, sexual preferences and medical conditions;
- 'privacy of location and space'
- 'privacy of association', e.g. being part of trade unions, political groups, or religious communities.[62]

Questions to be accounted for include what type of information is exchanged, and what would be the limits to what is strictly necessary for the defined purposes. A number of strategies may mitigate the privacy implications of sharing certain types of data. In discussing the information exchanged, it can be relevant, for instance, whether access to raw data has been limited,[63] whether data has been aggregated with information from other sources,[64] whether it is separated, encrypted, anonymized, etc.[65]

Access to information

Along with the scope of surveillance and the types of information exchanged, the question of access control touches on several issues within FISPs: who has access to information and personal data that are shared in FISPs, how is access legally and technically regulated, and is access minimized?

Firstly, in some cases, security clearance may be needed in order to grant access to information. Granting security clearance to private sector actors is not self-evident and multiple ways of going about this are imaginable. Consequently, one of the questions to be asked regarding access is on what basis private sector access to sensitive information is formally arranged.

Secondly, once security clearance is granted, what are the procedures in place for granting and withdrawing individuals' access to information?

Thirdly, depending on the type of collaboration, the exchange of information within FISPs may solely follow formal channels or may rely to varying degrees on informal exchanges of information. In the interests of transparency and accountability, questions can be raised regarding keeping records of access and information exchanges.

Further questions around access relate to the direction of information flows[66] and the timing of information exchange, such as whether information is exchanged in real time.[67]

Lastly, what are the protocols regarding the circulation of information within private sector institutions, e.g. between different branches of the same banking group, as well as for cross-border information sharing?

Data protection

The compatibility of financial transactions analysis with applicable data protection laws has been called into question on multiple fronts.[68] Public-private partnerships are subject to AML/CFT legislation on the one hand, and data protection and privacy laws on the other. These two regimes are sometimes in tension, which makes compliance challenging. Despite goodwill in the financial industry, privacy and data protection remain challenging to reconcile with AML/CFT operations.

60 Rogovin 1986
61 Amicelle & Favarel-Garrigues, 2012: p. 106
62 Finn, Wright, & Friedewald, 2013; Amnesty International, 2017: p. 28
63 E.g. through the use of Privacy Enhancing Technologies/privacy preserving analytics, see Maxwell, 2020
64 Zuboff, 2019
65 Many helpful strategies to improve privacy have been developed through the discussion on 'privacy by design'. See for instance: Hoepman, 2020; Cavoukian, 2009.
66 Maxwell & Artingstall, 2017: p. 35
67 Maxwell & Artingstall, 2017: p. 32
68 Purtova, 2018

This is partly due to a lack of expertise in the combined area, but mainly due to a lack of cooperation and alignment in the crafting of AML/CFT on the one hand, and privacy laws on the other. As a result, the implementation of data protection in AML/CFT compliance is considered to still be in its infancy.[69]

A second reason for concern about data protection is the blurred line between private and public entities. The distinction between government and private sector privacy obligations is fading as a result of private actors carrying out some functions that were previously the reserve of law enforcement.[70] This is reflected in issues of legal uncertainty surrounding public and private partnerships in the EU. Accountability structures for private companies are regulated differently than public ones, causing FISPs to fall within a grey area of GDPR. As the private and public sides of partnerships may be governed by different regimes of data protection, public-private partnerships are feared to risk lowering data protection standards.[71]

To ensure legal certainty in FISP operations, questions must be resolved regarding the regulatory framework within which it operates. Does the FISP fully comply with applicable privacy and data protection regulations? Is there a lack of clarity in terms of jurisdiction, applicable law, or unregulated aspects? Are certain aspects incompatible or within grey zones of privacy and data protection regulations – and if so, how are they resolved? Does the form the FISP takes risk lowering data protection standards? These questions relate to domestic legal contexts, but are magnified when information is shared across borders, or in the case of multi-jurisdictional FISPs.[72]

Data protection also raises questions about data retention and the length of storage of records about flagged transactions and individuals. Where and for how long is personal information and search records stored? For instance, touching on the data protection principle of 'the right to be forgotten',[73] are records being kept on individuals who have been cleared of suspicion?[74]

Data protection also relates to whether security of the data is adequately protected.[75] Have the dangers to the security of the data been identified? Which procedures and responsibilities have been put in place regarding data security? For instance, is there a safe environment for sensitive data and ensuring maximum confidentiality? Is there adequate protection against data breaches in how data is stored and when data is in transit, and is data disposed of in secure ways?[76] Who within the FISP is held responsible and accountable for retention and security?

One final question is whether FISPs have conducted a Privacy Impact Assessment (PIA), which is one way to map and mitigate privacy and data protection risks.[77]

Profiling

Analysis of personal data carries the risk of profiling on the basis of for example race, religion or political opinion. According to the EU Police Information Directive (which applies to sharing law enforcement information in the EU context), *"Profiling that results in discrimination against natural persons on the basis of special categories of personal data [racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership] shall be prohibited, in accordance with Union law."*[78]

69 Frasher & Agnew, 2016
70 Stanley & Steinhardt, 2003: pp. 7-8
71 Purtova, 2018
72 Europol, 2017.
73 Maxwell & Artingstall, 2017: p. 31
74 Lyon, 2014: p. 11
75 Maxwell & Artingstall, 2017: p. 37; Cavoukian, 2009: p. 4.
76 Cavoukian, 209: p. 4.
77 A PIA is a legal requirement under GDPR, but may not be in other domestic legal environments.
78 Directive (EU) 2016/680, 2016: Art. 11.3

Nonetheless, financial surveillance activities hold the potential for (un)conscious ethnic or religious bias and for racial profiling and discrimination.[79] According to David Lyon, institutionalized prejudice may spill over in categorization practices and become enshrined in them.[80] Not only do the blind spots caused by implicit or explicit bias risk inefficiency by excluding certain potential threats that do not fit the biased view, but the consequences of bias may also deprive, for instance, migrant communities of possibilities to send remittances,[81] or Muslim charities to carry out humanitarian aid.[82]

The profiling categories and mechanisms of inscription and removal often function as a 'black box' in security technologies.[83] Making these processes and technologies public would pose a security risk. Therefore, their careful control and review by established institutions is crucial. In the interest of legal certainty, however, any uncertainty created by these mechanisms must be reduced, e.g. in cases where charities are designated as problematic or suspicious from a CFT point of view and individuals may suffer grave consequences if they happen to make donations to these charities.[84] Conversely, there may be risks that only particular types of charities (based on religious affiliations) are marked as potentially suspect in the context of CFT.

There are emerging questions on the ethics of technology with respect to potential bias in AI and algorithmically-driven systems for detection. Supposedly 'neutral' technologies based on automated decision-making risk producing uneven and unequal outcomes.[85] The instructions given to automatic systems to provide the basis for judgements[86] should be critically examined, and policies must be put in place to detect and reduce the likelihood of bias in algorithmic design and execution,[87] such as in the data used to train algorithms.

Even if FISPs work with targeted leads and datasets, awareness of profiling risks remains crucial. FISPs use social network analysis to map networks of potential terrorist suspects, a method which carries the risk of exponential growth of data. There is a need for careful control of implicit and explicit biases to ensure that they do not result in damage to individuals or organisations which are disproportionately targeted, and conversely to prevent potential threats being disproportionately overlooked. Unintentional harms can be mitigated by identifying the risks of algorithmic or human bias throughout key moments of FISP operations, and ensuring adequate safeguards be put in place to mitigate these risks. These may include training and monitoring of personnel handling data, and critically questioning the methodology of risk-scoring and the theory of (ab)normality on which they are based. To prevent and remedy bias, the act of categorization must continually be challenged.[88]

Key questions on bias and profiling are firstly, how risk and (ab)normality defined and whether that definition leaves room for bias, and secondly, which safeguards are in place to minimize bias in subjective judgements of individuals as well as in automated systems.

79 de Goede, 2018; Amicelle & Iafolla, 2018; Atia, 2007; Helgesson, 2011
80 Amnesty International, 2017: p. 23
81 Amoore & de Goede, 2005: pp. 154-155
82 de Goede, 2018: pp. 4-5
83 Amicelle & Favarel-Garrigues, 2012
84 Atia, 2007
85 Lyon, 2014: p. 10
86 de Goede, 2018: pp. 16-17
87 de Goede, 2018; Lyon, 2014; Turner Lee, 2018
88 Atia, 2007: p. 463

Key questions
Cluster II: Privacy and proportionality

Scope

- Which factors influence the scale of data collection?
- Is the scope of data collection compatible with the principle of proportionality?

Nature of the information exchanged

- Which types of information are exchanged as part of the partnership?
- Does the level of intrusiveness of data collection respect the principle of necessity?

Access to information

- On what basis is private sector access to sensitive information formally arranged?
- What procedures are in place for granting and withdrawing individuals' access to information?
- Are formal records kept of each exchange of information?
- What are the protocols regarding the circulation of information within private sector institutions and across borders?

Data protection

- What is the relevant legal privacy and data protection regime that applies to the FISP?
- Are there unresolved questions in terms of jurisdiction, applicable law, or unregulated aspects?
- Does the FISP fully comply with privacy and data protection regulations, or are certain aspects incompatible or within grey zones of privacy and data protection regulations?
- Has a Privacy Impact Assessment been conducted?
- Where is data stored, and is the length of data storage minimized?
- Which dangers exist to the security of the data? Which procedures and responsibilities are put into place regarding data security?

Profiling

- How are risk and (ab)normality defined? Does this definition leave room for bias?
- Which safeguards are in place to minimize bias in subjective judgements of individuals as well as in automated systems?

III. MISTAKES AND MISUSE

FISPs hold a risk of producing adverse impacts when they are not used for the purpose or in the ways in which they were intended, or when their set-up is inherently flawed. What exactly constitutes misuse within any given FISP depends on how the aims, the legal obligations and ethical conduct have been defined. Misuse can manifest in many different ways and can be intentional or unintentional.

Any process, no matter how well embedded legally, can involve risks of mistakes and misuse which need to be reckoned with. What is at stake is limiting the implications of arbitrary and wrongful designation and protecting the rights of suspects and subjects whose information is shared. The purpose here is to help create awareness about these risks and set up the right mechanisms and procedures to minimize them.

Mistakes

Mistakes in the personal information shared within a FISP, as well as mistakes during the process of analysis within a FISP,[89] have the potential to cause harm. In the context of CFT, concerns have been raised regarding the frequency of false positives and of lists containing erroneous information.[90]

Concerns about mistakes mainly revolve around the degree of subjectivity associated with the suspicion process.[91] FISPs share personal information of persons who have come to the attention of law enforcement, but are not yet suspects in the legal sense (i.e. in the sense of being charged with a crime). In this manner, FISPs operate at the intersection between law enforcement and intelligence. It is imperative to guard against wrongful suspicion and the harms this may cause.

From a human rights perspective, these risks require careful attention, as the material harms inflicted on individuals affected by financial exclusion (account closures, asset freezes) are grave.[92] In the aftermath of the cases of Abdullah Kadi and Nabil Sayadi & Patricia Vinck, the harmful consequences to wrongly accused individuals have been extensively demonstrated.[93]

All systems can make mistakes, but the ethical question is how their occurrence and harmful consequences are recognised and minimized in a systematic way. Wrongful allocations can be the consequence of both human errors of judgement and of algorithmically generated results. As private sector employees are crossing over to the sphere of security,[94] specific attention must be paid to their accuracy of judgement. It must be noted that this places high demands on public and private actors to invest in preventive and remedying measures such as training and recruiting.[95] And that by avoiding the risk of false positives, there is a counterbalancing risk of producing false negatives.

Key questions regarding intelligence mistakes include: Are adequate procedures in place to prevent, detect and remedy the occurrence of mistakes? Are sufficient controls and oversight in place to ensure maximum data accuracy? How is the risk of mistakes covered in private sector employee training?

Unintentional misuse

Unintentional misuse constitutes transgressions of the boundaries defined in all other sections of this report, whereby the FISP is not used in the way it was intended. The difference with intentional misuse (see below) is that these transgressions do not happen for particular commercial, personal or political motives. For instance, consider the case whereby a bank is requested that information about an ongoing investigation is not shared with the client in question, but the client is *unintentionally* tipped off, whether directly

89 Guild, 2008
90 Amicelle & Favarel-Garrigues, 2012: p. 112
91 Amicelle & Iafolla, 2018
92 de Goede, 2018
93 Amicelle & Favarel-Garrigues, 2012: p. 110
94 Atia, 2007: p. 462
95 Helgesson, 2011

or indirectly. Or when a bank employee disregards an agreement that information may not be circulated freely with international branches of its company. Despite happening unintentionally or out of ignorance, this is nevertheless a breach of the access controls agreed upon or set down in law. These scenarios illustrate the need for clarity and adequate training on what are considered transgressions and thus what the legal requirements and ethical practice agreements are within the FISP.

Intentional misuse

Any system based on subjective and situated judgements on what can be deemed as unusual or suspicious, holds the potential for intentional misuse, or abuse.[96] Intentional misuse may take many forms.

Financial information sharing can be problematic when either private company employees or law enforcement personnel abuse their power for personal gain, political motives or commercial/strategic motives. This risk is linked to the issue of broad discretion in applying the definition of terrorism and of the categories of 'suspect' or 'unusual'. The lack of a universally accepted definition of terrorism[97] is known to leave a window for deliberate misuse of the term to target political opponents, human rights defenders, journalists, environmental activists and labour leaders.[98] As such, financial surveillance can be used as a tool for repression[99] or to serve the commercial interest of banks to exit certain clients.[100] It is therefore imperative that the criteria on which to base suspicion or unusual activity are objectively and uniformly determined, and that they are subject to careful control to ensure the necessary checks and balances are in place in their definition and their application.

Deliberate abuse may not always be straightforward. For instance, how are situations to be judged whereby certain information is held back because it is deemed commercially disadvantageous to the bank? In other cases, the difference between unintentional and intentional may be hard to distinguish. Consider, for instance, that a client is *intentionally* tipped off in the example whereby the bank is requested not to share information about ongoing investigations with the client in question.

The risk of misuse, whether intentional or unintentional, requires procedures to be in place to prevent, detect and remedy it. This necessitates transparency at all stages of the information-sharing activities. The points at which the FISP lends itself to misuse must be identified. This includes procedures to detect, flag and investigate misuse, but also requires clarity about what to do when there is suspicion of misuse. For instance, are banks to uncritically follow through on any information request, or do they have the power to refuse[101] sharing certain information when they are requested to, if they suspect or judge that there is misuse? As with mistakes, adequate training for private sector employees is required around issues of misuse.

96 de Goede, 2018
97 Sorel, 2003
98 Amnesty International, 2017: p. 23; Swire, 1999: p. 473
99 Martin, 2016: p. 27
100 Helgesson & Mörth, 2018; Favarel-Garrigues, Godefroy, & Lascoumes, 2011
101 Helgesson & Mörth, 2019

Key questions
Cluster III: Mistakes and misuse

Mistakes

- Are adequate procedures in place to prevent, detect and remedy the occurrence of mistakes?
- How is the risk of mistakes covered in private sector employee training?

Unintentional misuse

- What constitutes unintentional misuse within the FISP?
- Which procedures are in place to prevent, detect and remedy unintentional misuse?
- How is the risk of unintentional abuse covered in private sector employee training?

Intentional misuse

- What constitutes intentional misuse within the FISP?
- Which procedures are in place to prevent, detect and remedy intentional misuse?
- How is the risk of intentional abuse covered in private sector employee training?

IV. RIGHTS OF INDIVIDUALS

The fourth cluster of challenges identified in this report deals with the rights of individuals. We outline two sets of questions which may assess whether persons identified within a FISP are sufficiently protected and can find appropriate remedy.

Redress

Gary Marx, in his 'Ethics for the new surveillance',[102] underscores the need for appropriate means of redress when an individual has been unfairly treated or procedures violated. The issue of redress revolves around how irresponsible surveillance and violations can be remedied, and whether there is a forum to respond and grievances expressed. This includes whether suspects can challenge and contest decisions made regarding their personal information.

The EU Police Information Directive stipulates the right of the data subject to be informed of the purposes of data processes and to *"lodge a complaint with a supervisory authority and the contact details of the supervisory authority"*.[103]

The question of redress affects several human rights principles which have been confirmed in cases of UN and EU blacklisting (designations), including the right to an effective remedy set out in the European Convention on Human Rights, the right to a fair hearing and effective judicial protection,[104] as well as other principles such as the presumption of innocence,[105] transparency of procedures,[106] and the right to property.[107] The human rights implications associated with the absence of adequate and timely means of redress and judicial oversight following listing have been documented following several cases and remain an area of concern for human rights advocates.[108]

Questions to gauge the presence of adequate redress include whether affected persons are given sufficient information on procedures and decisions, including the reasons for being identified within a FISP and the authority which made the decision.[109] Additionally, if the individual has been treated unfairly or in cases where mistakes have been made, are there appropriate means of redress and judicial protection?[110]

De-risking

It is well known that de-risking is a harmful systemic consequence of CFT regulation and practices.[111] The FATF defines de-risking as *"the phenomenon of [...] restricting business relationships with [...] categories of clients to avoid, rather than manage, risk."*[112] De-risking is harmful especially if it affects certain groups more than others. Losing banking access has a major impact on an individual's or organization's life and effectively prevents societal and political participation.

FISPs pose a particular risk in the context of de-risking and generate specific questions concerning banks' responsibilities. In particular, it needs to be clear what happens to a suspect's banking access once they become identified within a FISP. In addition, the responsibility and liability of financial institutions which (continue to) provide banking services to a named suspect need to be clarified. Questions include whether protections against de-risking are in place; how suspects' banking access is protected, and what procedures have been agreed concerning the private partner's responsibilities and obligations towards suspects' banking access. If clients are exited from banking relations, are there means for redress (see above) and for clients to receive information concerning the bank's assessment and decision?

102 Marx, 1998
103 Directive (EU) 2016/680, Art. 13.1.d
104 Guild, 2008
105 Atia, 2007: p. 449
106 Amicelle & Favarel-Garrigues, 2012
107 Amicelle & Favarel-Garrigues, 2012: p. 110
108 Guild, 2008
109 Guild, 2008
110 Marx, 1998
111 Human Security Collective, 2018; Keatinge, 2014; Durner & Shetret, 2015; Duke Law International Human Rights Clinic and Women Peacemakers Program, 2017
112 FATF, 2014

Key questions
Cluster IV: Rights of individuals

Redress

- Are affected persons given sufficient information on procedures and decisions made as part of the FISP, regarding their data and assets?
- If the individual has been treated unfairly or in cases where mistakes have been made, are there appropriate means of redress and judicial protection?

De-risking

- What protections against de-risking are in place?
- How is suspects' banking access protected, especially when they are not accused or indicted?
- Have procedures been agreed concerning the private partner's responsibilities and obligations towards suspects' banking access, and the provision of information to clients whose banking relation has been terminated?
- Has bank liability been clarified and limited?

V. ACCOUNTABILITY

Ensuring accountability is important in a context where sensitive law enforcement information is passed between public and private spheres. FISPs, like other PPPs, operate at the intersection between the public and the private spheres. This poses particular challenges to the design of good accountability frameworks.[113] Oversight and accountability can help address some of the potential harms of profiling, mistakes and misuse discussed above. This section outlines four aspects of accountability, namely internal accountability, oversight, transparency and sanctions.

Internal accountability

Internal accountability considers the ways a FISP holds itself internally accountable for operating in alignment with ethical and privacy standards. This type of accountability requires that the partners in a FISP interrogate the partnership on the legal and ethical aspects described throughout this report. This may be achieved through conducting regular internal reviews and independent audits, and implementing corrective or complementary measures where necessary. Internal accountability implies a commitment to the continued improvement of policies and processes to safeguard proportionality and fundamental rights, and to detect and remedy any adverse effects such as mistakes, misuse and bias.

Oversight

A key contributing factor to the legitimacy of CFT measures is for the public to have confidence in the democratic oversight of the intelligence activities as they are happening.[114] This is not a straightforward task; in fact, *"finding the right level of government/public oversight of the intelligence community is one of the most important tasks facing any government"*.[115] External accountability of a FISP may be strengthened firstly through judicial oversight, and secondly by creating mechanisms for political accountability. Concerning other possible external oversight mechanisms, it needs to be questioned whether sufficient separation is ensured between the FISP participants and the oversight board or committee.

There are two main questions regarding oversight. Firstly, is the FISP subject to regulatory oversight? Secondly, how does the FISP ensure political accountability? This includes whether the FISP is evaluated through deliberative democratic forums based on regular external reporting, and whether the FISP is supported by broad citizens consent. For instance, are broad surveys conducted to gauge citizens' support and consent (e.g. Eurobarometer)? Are there indications of resistance against the measures (e.g. protest, press, social media)?[116]

Transparency

Transparency as a transversal principle is crucial to enable external accountability. How can the public have confidence in FISP activities if crucial decisions and operations remain invisible to them? Transparency on number of data shared and interventions made, is also of crucial importance for establishing the effectiveness of FISPs. As Maxwell and Artingstall note, *"transparency [of FISPs] can be provided by developing and publishing performance and impact metrics, as well as welcoming informed public policy debate around the use of the approach."*[117] The key question to be asked is: are the operations of the FISP sufficiently transparent so that they may continue to be subjected to public debate?

A clear way for FISPs to offer transparency is to regularly publish information about their activities. To date, FISPs offer some public reporting, but publicly available information concerning their operational aspects is limited, for example regarding the amount of data shared or the types of interventions made on the basis of their analysis. Therefore, questions regarding transparency gauge the extent of the information

113 Bures, 2012
114 Omand & Phytian, 2013: p. 58
115 Pateman, 2003
116 Steinfeld, 2017
117 Maxwell & Artingstall, 2017: p. 36

included in reporting, for instance whether information about it entails ethical and legal aspects. Secondly, they touch on which publics the reporting is made available to. Is access to this information limited to certain groups of people, and what are the thresholds for access? In other words, is the information easily available?

Evidently, the very nature of intelligence activities requires a certain level of secrecy. However, what constitutes 'appropriate secrecy' must be justified and continually challenged.[118] Therefore, if there is a need to keep aspects of the FISP secret, is that secrecy explained and justified?

Sanctions

From the question of sufficient oversight flows the question of which sanctions are in place, because to be meaningful all forms of accountability rely on the threat of consequences for transgressions. The question of sanctions is twofold. Firstly, what procedures are in place to penalize and amend transgressions such as mistakes, misuse or bias? Secondly, what consequences are attached to the FISP or its members if they fall short of respecting fundamental rights, proportionality or ethical standards?

118 Diderichsen & Ronn, 2017

Key questions
Cluster V: Accountability

Internal accountability

- How does the FISP hold itself internally accountable for operating in alignment with ethical standards?

Oversight

- Are FISP activities subject to regulatory oversight?
- How does the FISP ensure political accountability?
- Is the FISP supported by broad citizens consent?

Transparency

- Does the FISP regularly publish information about its activities, and does this include information about its ethical and legal aspects?
- To which publics is reporting made available?
- Are the operations of the FISP sufficiently transparent so that they may continue to be subjected to public debate?
- If there is a need to keep aspects of the FISP secret, how is that secrecy explained and justified?

Sanctions

- What procedures are in place to penalize and amend transgressions such as mistakes, misuse or bias?
- What consequences are attached to the FISP or its members if they fall short of respecting fundamental rights, proportionality or ethical standards?

CONCLUSION

This report has collected an overview of the ethical and legal challenges of targeted financial data sharing as part of Financial Intelligence-Sharing Partnerships (FISPs).

FISPs are relatively new forms of public-private partnerships. They enable proactive sharing of personal information between law enforcement and private institutions. While these types of partnerships can be more effective than traditional CFT approaches, they raise considerable questions concerning their legal basis, privacy protections and the rights of suspects, which have been insufficiently analysed to date.

This report has given an extensive overview of legal and ethical challenges relating to FISPs and to financial surveillance more broadly. We have identified five clusters of questions relating to (I) democratic legitimacy, (II) privacy and proportionality, (III) mistakes and misuse, (IV) rights of individuals and (V) accountability. Together, we outline 47 thought-provoking questions about financial surveillance in general, applied to FISPs. The questions are designed to draw the attention of FISP participants to the ethical and legal dimensions of their practice and help assess whether the activities of FISPs are consistent with ethical and legal standards. We propose that these questions be used to foster a conversation and to assess FISP practices in the context of good governance. Addressing these questions will be a way for FISPs to strengthen their legitimacy and basis for future development.

In the next phase of this research, we will build on the 47 questions outlined here to examine FISPs in practice. We will study how the practices of selected FISPs deal with the questions outlined in this report, in order to identify best practices. Eventually, our research will culminate in a report on best practice and policy recommendations for FISPs.

ANNEX 1: KEY QUESTIONS OVERVIEW

Cluster I: Democratic legitimacy

Establishment process

- Was the FISP established through democratic decision-making procedures?
- Was the decision to set up the partnership subject to public discussion and political deliberation prior to its start?

Legal basis

- What is the legal basis of the FISP?
- Is the legal basis of the FISP grounded in existing law or through enabling legislation drafted with the explicit purpose of creating the FISP?

Necessity

- Has the need for a FISP as an alternative or addition to the existing CFT regime been demonstrated?

Composition

- On what basis are decisions made regarding which institutions to include in the partnership?
- Does the inclusion of certain private sector institutions produce a competitive disadvantage towards excluded institutions, or vice versa?

Legitimate aim

- How are the objectives of the partnership defined and justified?
- To what extent do the boundaries of its purpose allow for flexibility?

Cluster II: Privacy and proportionality

Scope

- Which factors influence the scale of data collection?
- Is the scope of data collection compatible with the principle of proportionality?

Nature of the information exchanged

- Which types of information are exchanged as part of the partnership?
- Does the level of intrusiveness of data collection respect the principle of necessity?

Access to information

- On what basis is private sector access to sensitive information formally arranged?
- What procedures are in place for granting and withdrawing individuals' access to information?
- Are formal records kept of each exchange of information?
- What are the protocols regarding the circulation of information within private sector institutions and across borders?

Data protection

- What is the relevant legal privacy and data protection regime that applies to the FISP?
- Are there unresolved questions in terms of jurisdiction, applicable law, or unregulated aspects?
- Does the FISP fully comply with privacy and data protection regulations, or are certain aspects incompatible or within grey zones of privacy and data protection regulations?
- Has a Privacy Impact Assessment been conducted?
- Where is data stored, and is the length of data storage minimized?
- Which dangers exist to the security of the data? Which procedures and responsibilities are put into place regarding data security?

Profiling

- How are risk and (ab)normality defined? Does this definition leave room for bias?
- Which safeguards are in place to minimize bias in subjective judgements of individuals as well as in automated systems?

Cluster III: Mistakes and misuse

Mistakes

- Are adequate procedures in place to prevent, detect and remedy the occurrence of mistakes?
- How is the risk of mistakes covered in private sector employee training?

Unintentional misuse

- What constitutes unintentional misuse within the FISP?
- Which procedures are in place to prevent, detect and remedy unintentional misuse?
- How is the risk of unintentional abuse covered in private sector employee training?

Intentional misuse

- What constitutes intentional misuse within the FISP?
- Which procedures are in place to prevent, detect and remedy intentional misuse?
- How is the risk of intentional abuse covered in private sector employee training?

Cluster IV: Rights of individuals

Redress

- Are affected persons given sufficient information on procedures and decisions made as part of the FISP, regarding their data and assets?
- If the individual has been treated unfairly or in cases where mistakes have been made, are there appropriate means of redress and judicial protection?

De-risking

- What protections against de-risking are in place?
- How is suspects' banking access protected, especially when they are not accused or indicted?
- Have procedures been agreed concerning the private partner's responsibilities and obligations towards suspects' banking access, and the provision of information to clients whose banking relation has been terminated?
- Has bank liability been clarified and limited?

Cluster V: Accountability

Internal accountability

- How does the FISP hold itself internally accountable for operating in alignment with ethical standards?

Oversight

- Are FISP activities subject to regulatory oversight?
- How does the FISP ensure political accountability?
- Is the FISP supported by broad citizens consent?

Transparency

- Does the FISP regularly publish information about its activities, and does this include information about its ethical and legal aspects?
- To which publics is reporting made available?
- Are the operations of the FISP sufficiently transparent so that they may continue to be subjected to public debate?
- If there is a need to keep aspects of the FISP secret, how is that secrecy explained and justified?

Sanctions

- What procedures are in place to penalize and amend transgressions such as mistakes, misuse or bias?
- What consequences are attached to the FISP or its members if they fall short of respecting fundamental rights, proportionality or ethical standards?

ANNEX 2: SOURCES CITED

ACLU. (2009). *Blocking Faith, Freezing Charity: Chilling Muslim Charitable Giving in the "War on Terrorism Financing"*. New York: American Civil Liberties Union.

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

Amicelle, A., & Iafolla, V. (2017). *Reporting Suspicion in Canada: Insights from the fight against money laundering and terrorist financing.* Montréal: Canadian Network for Research on Terrorism, Security and Society.

Amicelle, A., & Iafolla, V. (2018). Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing. *British Journal of Criminology, 58*(4).

Amnesty International. (2017). *Dangerously disproportionate: The ever-expanding national security state in Europe.*

Amnesty International. (2019). *Ending the targeted digital surveillance of those who defend our rights: a summary of the impact of the digital surveillance industry on human rights defenders.*

Amoore, L., & de Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change, 43*(2-3), 149-173.

Andrew, J., & Baker, M. (2019). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*.

Anwar, T. (2020). Unfolding the past, proving the present: social media evidence in terrorism financing court cases. *International Political Sociology, 14*, 382-398.

Atia, M. (2007). In whose interest? Financial surveillance and the circuits of exception in the war on terror. *Environment and Planning D: Society and Space, 25*, 447-475.

Büchi, L., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law and Security Review, 36*.

Bures, O. (2012). Private Actors in the Fight Against Terrorist Financing: Efficiency Versus Effectiveness. *Studies in Conflict & Terrorism, 35*(10), 712-732.

Cavoukian, A. (2009). *Privacy by design: the 7 foundational principles. Implementation and mapping of Fair Information Practices.*

Chong, A. (2020). (Self-)Regulation of Muslim charitable sectors in the US and the UK in the post-9/11 era. *Journal of Muslim Philanthropy & Civil Society, 4*(1).

Clearinghouse (2017). A New Paradigm: Redesigning the US AML/CFT Framework to protect National Security and Aid Law Enforcement, February.

Davis, J. (2020). *New Technologies but Old Methods in Terrorism Financing.* CRAAFT.

de Goede, M. (2014). Preemption contested: Suspect spaces and preventability in the July 7 inquest. *Political Geography, 39*, 48-57.

de Goede, M. (2018). The Chain of Security. *Review of International Studies, 44*(1), 24-42.

de Goede, M. & Sullivan, G. (2016). The politics of security lists. *Environment and Planning D: Society and Space, 34*(1), 67-88.

de Oliveira, I. (2016). *Challenges to Information Sharing: Perceptions and Realities.* RUSI.

Diderichsen, A., & Ronn, K. (2017). Intelligence by consent: on the inadequacy of Just War Theory as a framework for intelligence ethics. *Intelligence and National Security, 32*(4), 479-493.

Directive (EU) 2016/680 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 (2016). *Official Journal of the European Union*, L119/189.

Duke Law International Human Rights Clinic and Women Peacemakers Program. (2017). *Tightening the Purse Strings: What Countering Terrorism Financing Costs Gender Equality and Security.*

Durner, T. & Shetret, L. (2015). *Understanding Bank De-Risking and its Effects on Financial Inclusion*. Global Center on Cooperative Security.

Etzioni, A. (2018). Apple: Good Business, Poor Citizen? *Journal of Business Ethics, 151*(1).
European Data Protection Supervisor. (2020, January 28). *The EDPS quick-guide to necessity and proportionality*. Retrieved from EDPS: https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quickguide_en.pdf
Europol (2017) *From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact*. Luxembourg: Publications Office of the European Union.
FATF. (October 23, 2014). *FATF clarifies risk-based approach: case-by-case, not wholesale-derisking*. Retrieved from FATF: http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html
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.
Finn, R., Wright, D., & Friedewald, M. (2013). Seven types of privacy. *European Data Protection: Coming of Age*, 3-32.
Frasher, M. (2013). Violence, law and culture: The social construction of US and European privacy identities and transatlantic counter-terrorism cooperation. *ROCZNIKI KULTUROZNAWCZE, 4*(2).
Frasher, M., & Agnew, B. (2016). *Multinational Banking and Conflicts among US-EU AML/CTF Compliance & Privacy Law: Operational & Political Views in Context.* SWIFT Institute.
Gould, C. (2019). How democracy can inform consent: Cases of the internet and bioethics. *Journal of Applied Philosophy, 36*(2), 173-191.
Guild, E. (2008). The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the 'Terrorist Lists'. *JCMS, 46*(1), 173-193.
Helgesson, K. (2011). Public-Private Partners Against Crime: Governance, Surveillance and the Limits of Corporate Accountability. *Surveillance & Society, 8*(4).
Helgesson, K., & Mörth, U. (2018). Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention. *Crime, Law and Social Change, 69*(2), 227-248.
Helgesson, K., & Mörth, U. (2019). Instruments of securitization and resisting subjects: For-profit professionals in the finance–security nexus. *Security Dialogue, 50*(3), 257-274.
Hoepman, J. (2020, January 27). *Privacyontwerpstrategieën (Het Blauwe Boekje).* Retrieved from Radboud University: https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf
Hufnagel, S., & King, C. (2020). Anti-Money Laundering Regulation and the Art Market. *Legal Studies.*
Human Security Collective. (2018). *At the Intersection of Security and Regulation: Understanding the Drivers of Derisking and Civil Society Organizations*, The Hague, March.
Keatinge, T., & Keen, F. (2020). *A Sharper Image: Advancing a Risk-Based Response to Terrorist Financing.* RUSI.
Keatinge, T. (2014). Uncharitable behaviour: Counter-terrorist regulation restricts charity banking. *Demos.*
King, K., Walker, C., & Gurulé, J. (2018). *The Palgrave Handbook of Criminal and Terrorism Financing Law.* Palgrave Macmillan.
Lyon, D. (2003). Surveillance After September 11. Polity Press.
Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society, 1*(2).
Macnish, K. (2014). Just Surveillance? Towards a Normative Theory of Surveillance. *Surveillance & Society, 12*(1), 142-153.
Martin, K. (2016). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics, 137*(3), 551-569.
Marx, G. (1998). Ethics for the new surveillance. *Information Society, 14*(3), 171-185.
Maxwell, N. (2019). *Expanding the Capability of Financial Information-Sharing Partnerships.* RUSI.
Maxwell, N. (2020). *Case studies of the use of privacy preserving analysis to tackle financial crime.*

Maxwell, N. (2020). *Five years of growth in public–private financial information-sharing partnerships to tackle crime.* FFIS.
Maxwell, N. (2020). *Future of Financial Intelligence Sharing (FFIS) research programme: Five years of growth in public–private financial information-sharing partnerships to tackle crime.* RUSI.
Maxwell, N., & Artingstall, D. (2017). *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime.* London: RUSI.
OECD. (n.d.). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from OECD: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacy-andtransborderflowsofpersonaldata.htm
Omand, S., & Phytian, M. (2013). Ethics and intelligence: A debate. *International Journal of Intelligence and Counterintelligence, 26*(1), 38-63.
Opitz, S. & Tellmann, U. (2014). Future Emergencies: Temporal Politics in Law and Economy. *Theory, Culture & Society, 32*(2), 107–29.
Parker, M., & Taylor, M. (2011). Financial Intelligence: A Price Worth Paying? *Studies in Conflict & Terrorism, 33*(11), 949-959.
Pateman, R. (2003). *Residual Uncertainty: Trying to Avoid Intelligence and Policy Mistakes in the Modern World.* University Press of America.
Purtova, N. (2018). Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships. *International Data Privacy Law, 8*(1), 52-68.
Reidenberg, J. (2001). E-commerce and Trans-Atlantic Privacy. *Houston Law Review, 38*, 717-749.
Roessler, B. (2017). Privacy as a human right. *Proceedings of the Aristotelian Society, 117*(2), 187-206.
Rogovin, M. (1986). Privacy of Financial Records. *Annual Survey of American Law, 3*, 587-608.
Ross, S., & Hannan, M. (2007). Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control, 10*(1), 106-115.
Roth, J., Greenberg, D., & Wille, S. (2019). *9/11 Monograph on Terrorist Financing: Staff Report of the National Commission on Terrorist Attacks Upon the United States.*
Sharman, J. (2009). Privacy as roguery: Personal financial information in an age of transparency. *Public Administration, 87*(4), 717-731.
Sorel, J. (2003). Some Questions About the Definition of Terrorism and the Fight Against Its Financing. *European Journal of International Law, 14*(2), 365-378.
Stanley, J., & Steinhardt, B. (2003). *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society.* ACLU.
Steinfeld, N. (2017). Track me, track me not: Support and consent to state and private sector surveillance. *Telematics and Informatics, 34*, 1663-1672.
Swire, P. (1999). Financial Privacy and the Theory of High-Tech Government Surveillance. *Washington University Law Quarterly, 77*(2), 461-512.
Turner Lee, N. (2018). Detecting racial bias in algorithms and machine learning. *Journal of Information, Communication and Ethics in Society, 16*(3), 252-260.
Wesseling, M. & de Goede, M. (2018). *Beleid bestrijding terrorismefinanciering: effectiviteit en effecten (2013-2016).*
Wright, D. (2011). A framework for the ethical impact assessment of information technology. *Ethics Inf Technol, 13,* 199–226.
Wright, D., Rodrigues, R., Raab, C., Jones, R., Székely, I, Ball, K., Bellanova, R., Bergersen, S. (2015). Questioning Surveillance. *Computer Law & Security Review, 31*(2), 280-292.
Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Profile Books Ltd.