Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Challenges to Information Sharing

Perceptions and Realities

Inês Sofia de Oliveira

Challenges to Information Sharing

Perceptions and Realities

Inês Sofia de Oliveira

RUSI Occasional Paper, July 2016

Royal United Services Institute
for Defence and Security Studies

Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK's leading independent think-tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, July 2016 ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Foreword

Like clockwork, following each and every terrorist attack that has occurred in recent times, global leaders call for greater information sharing to counter the threat of terrorists and their financing. Strategies to tackle money laundering, such as that recently announced in the UK, are built upon the belief that greater information sharing is the means by which nations can achieve a step-change in the fight against financial crime, and the financial sector continuously demands feedback and guidance from the authorities in order to meet the financial crime identification and disruption challenges that are put upon them. Information sharing is viewed almost universally as the critical determinant of success.

Yet the meaningful and effective sharing of information remains elusive. Privacy and data protection concerns prevail; regulation is poorly understood; and banks' policies and procedures often place client confidentiality and discretion at the heart of business strategy. Balancing these two competing positions continues to vex policy-makers and practitioners alike.

This latest paper from RUSI's Centre for Financial Crime and Security Studies seeks to unpack the perceptions and realities of information sharing, identifying where such exchanges are, for example, permitted in the name of security; how legislation can enhance the ability of information to be shared on an effective basis, including between private sector entities; how guidance from national authorities can improve the quality of information provided by the private sector to the public sector; and how the concepts of necessity and proportionality should govern decision-making, balancing a heightened focus on security with continued data protection and privacy.

The focus of this paper is on understanding 'the art of the possible' in the field of information sharing, identifying genuine barriers where they exist, and considering how changes to legislation could be made that enable not *more*, but *better* information sharing to increase the effectiveness of current approaches to tackling terrorist financing and financial crime.

Tom Keatinge
Director, Centre for Financial Crime and Security Studies, RUSI
July 2016

Executive Summary

NO HIGH-LEVEL GATHERING addressing the problem of financial crime and terrorism financing is complete without calls for greater information sharing in the interests of security against the growing threat posed to Western nations by terrorist activity, particularly that of Daesh (also known as the Islamic State of Iraq and Syria, ISIS or IS). Yet these calls for information exchange, including financial information, are often frustrated by concerns about data protection and privacy. Addressing the UN Security Council in December 2015, Je-Yoon Shin, the president of the Financial Action Task Force (FATF), observed that 'different data protection laws mean that one of our largest sources of intelligence, the banks, are often prevented from sharing information across borders within their own organisations, let alone with each other or with the authorities'.[1] Yet the championing of security interests over those of data protection has received support from some unlikely quarters as the threat of terrorism in Europe has risen in recent months. Speaking on German television, the German interior minister, Thomas de Maizière, said that 'data protection is all very well, but in times of crisis, security has priority'.[2]

In the area of financial crime, the interplay between the interests of anti-money laundering and counter-terrorist financing (AML/CTF) and those of data protection is also increasingly questioned by public and private sector actors. Some believe there is increasing potential for conflict between the two as calls for information sharing expand.

The EU and the UK have recently revised and strengthened the AML/CTF regime through the adoption of the 2012 Recommendations of the FATF.[3] This is reflected in the EU's Fourth AML Directive, which the European Commission wants to see implemented by the end of 2016. A new EU data-protection regime has also been approved, consisting of a General Data Protection Regulation (GDPR) 'on the protection of natural persons with regard to the processing of personal data and on the free movement of such data' and a Data Protection Directive (DPD) 'on the protection of natural persons with regard to the processing of personal data by competent

1. Je-Yoon Shin, 'The Importance of Urgent Action to Implement FATF's Measures to Counter Terrorist Financing and Help Defeat ISIL', speech at the UN Security Council, New York, 17 December 2015.
2. 'Datenschutz ist schön, aber in Krisenzeiten hat Sicherheit Vorrang', (author translation), from *Tagesschau, '*De Maizière will an die "Datentöpfe"', 22 March 2016.
3. For the purposes of this paper the UK and EU frameworks are interchangeable, since the UK is obliged to follow EU law. While the FATF defines the AML/CTF requirements, their implementation is subsequently transformed into law by individual states. Within the EU, FATF standards are adopted at EU and member state level simultaneously. EU directives establish a lowest common denominator which must be adopted by all states. However, both EU directives and individual states sometimes introduce measures that extend beyond FATF requirements to better facilitate the functioning of the internal market and to adjust to specific realities. The conflict under analysis in this paper is best considered from the perspective of the EU, highlighting the UK as a case study of national implementation.

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'. Both are due to be implemented in the UK soon.

But do the existing requirements on states and their regulated sectors actually conflict with data protection regulations? Or do the calls to expand information sharing and public-private partnership threaten to create such a conflict, one that should be anticipated and provided for in law?

This paper begins by considering the potential for conflict between the two existing frameworks. It suggests that the primary issue for those concerned with data protection and privacy is significant over-reporting by a regulated sector that, seeking to learn from the numerous regulatory actions and fines against it in recent years, and lacking guidance from the authorities, is apparently incentivised to file a glut of unfocused, poor-quality information with the authorities in an effort to protect itself from further censure and penalty. Using the UK as a case study, this paper suggests that the challenges facing the status quo arise not from current information-sharing requirements but from the volume of data gathered in compliance with the FATF's Recommendations, which conflicts with the concepts of 'necessity' and 'proportionality' that underpin data-protection legislation.

This paper suggests that, *ceteris paribus*, there is no apparent conflict between data protection and financial crime regulation under the current frameworks. Existing processes used by the private and public sectors – through which data are collected, processed and ultimately deleted – are, however, deemed to be ineffective and are widely criticised. The challenge lies in attempts to implement a more effective information-sharing system which operates within the constraints of both information-sharing and data protection imperatives.

This paper considers this conflict in the context of the called-for expansion of information sharing in light of recent terrorist attacks in particular, and the fight against transnational illicit finance more generally. It is here, as authorities seek to integrate national financial data across borders and place greater onus on the private sector, that conflict is identified and should be addressed in a manner consistent with EU requirements for 'necessity' and 'proportionality'.

This paper's discussion of the relationship between data protection and AML/CTF reflects the broader challenges that security concerns present to individual privacy and to businesses required to implement financial crime and data-protection regulation at an operational level. It determines that, while there is some potential for conflict under existing frameworks, the need for change derives from new requests for expanded information-sharing capabilities in response to the identification of legislative gaps, rather than from any deficiency in current regulation.

Greater engagement by the public sector is thus needed to ensure that the information shared is relevant and is processed and used or dismissed in a timely manner by the appropriate actors. This could be achieved by widening private sector powers to share information voluntarily in

cases where there is reason to suspect criminal activity, leading to improved quality, greater relevance and reduced quantities of data filed.

This paper proposes the following recommendations to ensure that increased information sharing is developed in a manner consistent with the concepts of 'necessity' and 'proportionality', balancing a heightened focus on security with continued data protection and privacy:

1. Current regulations need to be clarified and supplemented with additional guidance, in response to concerns expressed by the private sector that they are confusing and difficult to understand, so that information sharing is maximised under existing frameworks.
2. State authorities should provide better guidance to their regulated sectors so that the excessive quantities of data submitted by those sectors and retained by law enforcement can be reduced, in line with the concepts of 'necessity' and 'proportionality'.
3. Legislation should allow for private-to-private information sharing in accordance with the principles of 'necessity' and 'proportionality'.
4. Consideration should be given to expanding the role and 'competences' of the private sector in tackling financial crime, particularly in the light of increasing expectations that its involvement in the disruption of financial crime is likely to expand. This should include the possibility of voluntary information sharing.
5. The private sector should revise data protection policies and safeguards to assure clients that information collected to tackle financial crime is not used for other purposes.

A brief note on scope. While the cross-border nature of financial crime means that an examination of non-EU jurisdictions is appropriate, the sharing of data beyond the EU is complicated by the diversity of safeguards on offer. The research presented here is thus focused on the nexus of information sharing and data protection within the UK and the EU.

This research was carried out prior to the results of the UK's referendum on its membership of the EU. Despite the obvious consequences that a departure from the Union will have on any upcoming legislation, it is unlikely that regulations and obstacles, as discussed in this paper, will be signficantly different, especially since the majority of these are already in place. Furthermore, as requirements to fight financial crime are international in nature, states must, regardless of their membership of multilatral bodies, implement them. Finally, as with other non-EU countries, if the UK wishes to continue trading with the EU and accessing the single market, it will be required to implement data-protection and AML requirements as per EU law.

Perceptions and Realities: Data Protection as an Obstacle to Information Sharing

THE EVENTS OF 11 September 2001 (9/11) put in motion a series of policy initiatives to restrict the access of terrorist groups and their supporters to the financial system, to track their movements, networks and recruitment, and reduce the likelihood of future attacks – all measures that presented challenges to individual privacy and data protection.

The relationship between data protection, counter-terrorism and other types of serious crime has, for some time, been under review at domestic and international levels. The process has involved significant co-operation between different jurisdictions and their policy, law enforcement and private sector actors. The debate around Passenger Name Records is a case in point.[1]

In practice, the stepping-up of security-oriented international policies means that states are allowed to restrict some individual rights – for example, the right to privacy – in specific situations where access to information could be conducive to public safety, national security or the disruption of crime. State authorities are therefore able to access data such as individual communications, travel records and financial transactions.

To do this effectively, state authorities have become reliant on the co-operation and contribution that the private sector – in particular, financial institutions – is able to provide. Given the extensive information such businesses gather on the actions of individuals via their everyday operations, they inevitably regularly confront the security/data-protection debate.

The private sector may share personal data with the authorities in cases where there is suspicion of a crime. Private sector actors in regulated industries are required to monitor for suspicious activity, recording transactions and reporting them to the appropriate authorities in case of doubt or suspicion of illegality. Authorities are then responsible for investigating these suspicions and at times requesting further information from the reporting entities. Throughout this process, the suspects (individuals or organisations) must remain unaware of the monitoring, reporting or investigation to avoid influencing their actions ('tipping off') or interfering with the normal course of justice.

The global, and generally accepted, AML/CTF framework – as set by the FATF – is a crucial example of a system where data protection and security frameworks meet. Law enforcement, policy-makers and private sector actors work tirelessly to ensure FATF standards are implemented in

1. Cécile Barbière, 'MEPs Refuse to Vote on PNR before Council Strengthens Data Protection', *EurActiv*, 9 March 2016.

a manner consistent with business priorities, but also in furtherance of efforts to ensure public safety and tackle crime.

Despite best intentions, questions about the compatibility of financial crime regulation and data protection continue to arise. Systems, regulations and processes that have grown up over the past ten to fifteen years have been reactive and rarely anticipate the direction of technology or financial activity. At a time when calls for greater information sharing as part of the global CTF effort are getting louder, this paper seeks to bring clarity to an area where perception often conflicts with reality and where a clear assessment of the status quo is required so that the necessary improvements can be developed. It aims to do so through an analysis of the existing UK framework on financial crime as well as the relevant data-protection provisions (as reflected in EU standards).[2]

The analysis relies on interviews with private and public sector stakeholders, policy-makers and experts. These are corroborated by the literature and ongoing debates. It begins by identifying the data-protection framework, existing exemptions to tackling crime and its coexistence with AML/CTF requirements. This debate leads to the identification of the source of conflict between the two frameworks and elaborates on how a new information-sharing system could challenge existing practices. This paper then reflects on the need to consider the principles of 'necessity' and 'proportionality' in the making and implementation of both AML/CTF and data-protection frameworks and any revisions to them. Lastly, it makes a few suggestions on how to move forward.

Data Protection in the EU and the UK: The Status Quo

The principles of data protection are set out in the EU Data Protection Directive (95/46/EC), which has been transposed into member states' laws according to national criteria. The governing legislation in the UK is the Data Protection Act (DPA) 1998, whose eight main principles, set out in Schedule 1, state that personal data must be processed fairly and lawfully, for specified purposes, be adequate, relevant and not excessive, not kept longer than needed, kept secure, and not transferred out of the European Economic Area unless adequately protected.[3]

2. For simplification, this paper follows the wording and provisions set in EU law, as it provides the minimum common denominator for data protection in the EU, specifically the provisions contained in: European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' [hereafter GDPR], COM(2012) 11 final, 2012/0011 (COD), 25 January 2012; and European Commission, 'Proposal for a Directive of the European Parliament and of the Council 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', COM(2012) 10 final, 2012/0010 (COD), 25 January 2012. As regards the requirements for sharing information within the domestic context of criminal investigations and other exemptions, the paper applies UK law, namely the 2007 Anti-Money Laundering legislation and the 1998 UK Data Protection Act to provide a more accurate discussion.
3. There are eight data protection principles in practice in the UK, mirroring the EU Directive.

However, data protection is not an absolute right and is restricted by most jurisdictions, including the UK, in cases of threat to national security and for the investigation of criminal offences.[4] In the UK, these exemptions are provided for in S.28 (national security) and S.29 (crime and taxation) of the DPA, defining the legitimate limitations to the application of the data-protection principles.

S.28 necessarily imposes the greatest restriction on data protection, given its implications for national security. Where the exemption is engaged, those individuals whose data is processed lose their rights under the DPA, and the data controller is exempted from data protection principles. However, application of the exemption beyond competent authorities, such as the security and intelligence services, is a matter of fierce debate.

Where individuals are investigated for criminal offences (including money laundering, terrorist financing and tax evasion) and the S.29 exemption is engaged, they lose the right to be notified that their data are being processed or to prevent access to that data. However, they retain their other rights and the data controller remains subject to the rest of the data-protection principles.[5]

At EU level, exemptions or restrictions to data-protection provisions were recently revised by member states, in Article 21 of the EU's General Data Protection Regulation (GDPR) and the accompanying DPD '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'.[6] This was approved by the Council of the EU in December 2015 and confirmed by a European Parliament vote on 14 April 2016, although the revisions have not yet been

4. See Article 21 of the proposed EU Regulation (the GDPR). See the latest revised version at: <http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/>, accessed 23 June 2016.
5. Schedules 1, 2 and 3 set out the terms and conditions under which data can be processed and should be read in parallel to the DPA articles. They refer to the 'data protection principles', 'the conditions relevant for purposes of the first principle: processing of any personal data' and 'the conditions relevant for purposes of the first principle: processing of sensitive personal data' respectively.
6. EU law on data protection was initially defined under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. See European Parliament and Council, 'On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data', *Official Journal of the European Commission* (L 281, 23 November 1995), pp. 31-50. Restrictions to data protection were set in Article 13. As of December 2015, data protection provisions are set out in the GDPR. The regulation should be read in conjunction with another EU Directive: European Commission, 'Proposal for a Directive of the European Parliament and of the Council 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'.

implemented.[7] Areas exempt from the GDPR, considered by Article 21 to be necessary and proportionate in a democratic society, are reproduced in Box 1 below.

Box 1: Extracts from Article 21 of the EU GDPR

a. Public security;
b. The prevention, investigation, detection and prosecution of criminal offences;
c. Other public interests of the Union or of a Member State, in partiuclar an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;
d. The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
e. A monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c), (d);
f. The protection of the data subject or the rights and freedoms of others.

The exemptions set out in Article 21 do not include national security, as this is a matter for each member state. However, it is generally acknowledged that national security takes priority over data-protection rights where necessary.

Article 21 has direct relevance for UK law and will soon replace the exemptions in Part IV of the 1998 DPA, including the S.29 crime exemption, which reflects the permissions of the EU 1995 DPD, Article 13.[8]

Article 9 of the GDPR limits the processing of data relating to criminal convictions or related security measures, providing that they are carried out 'either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, *or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards'* (emphasis added by the author). Voluntary sharing of information by entities other than those referred to here, or under their supervision, is a challenge but is not impossible, as demonstrated in this paper.

Data Protection and Financial Crime

Combating financial crime and terrorist finance in accordance with adopted international standards is essential to states' maintenance of economic stability and the integrity of the

7. *European Parliament News*, 'Data Protection Reform – Parliament Approves New Rules Fit for the Digital Era', 14 April 2016.
8. European Parliament and Council, 'On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data', pp. 31–50.

financial system. These obligations broadly consist of information sharing through the monitoring of transactions and their reporting to authorities. In the context of AML/CTF, the use of financial intelligence (FININT) – information gathered through the monitoring of financial transactions for purposes of prevention, investigation or prosecution of crime and terrorist activities – is becoming increasingly important to law enforcement, public security and financial institutions carrying out risk assessments. As a result, existing data-protection exemptions are becoming more useful than ever.

FININT reveals patterns that potentially illustrate the preferences, habits and movements of the users of regulated financial systems. Its utility has gained momentum, but there is recognition of the need for balance with data protection imperatives. Clearly, FININT cannot be hindered to the point of uselessness by limitations imposed by the principles of data protection, but neither should its evolution outpace the associated and legally mandated provisions for data sharing, retention and access.

In the implementation of both frameworks, a balance must be struck between the need to safeguard against crime and threats to national security and the need to respect the principles of data protection. While legally mandated exemptions to data protection apparently facilitate the coexistence of both regimes today, the expansion of efforts to tackle financial crime through greater information sharing via new and existing mechanisms brings into question the continued symbiosis of the existing frameworks.

Before addressing how this conflict might materialise and how it might be resolved, it is important to consider the key EU principles of 'necessity' and 'proportionality' and their restraint on the application of current legislation.

Challenges and Conflicts in Applying Current Legislation

Sharing and Processing Data

While existing financial crime and data-protection frameworks appear to coexist without conflict, the burden placed on the private sector to contribute to fighting crime through the strict monitoring and reporting of any suspicious activity appears – at least in the UK, given the size of its financial system and its struggles to monitor suspicious activity[9] – to challenge current data-protection legislation.

The FATF's 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' – or FATF Recommendations – were revised in 2012 and are the core principles guiding data sharing in AML/CTF policies and regulations. Recommendations 20 and 21 define respectively the obligations to report suspicious activity and prohibit the disclosure of such reporting activity to the subject in question.

9. David Pegg, 'UK Banks at High Risk of Exposure to Laundered Money, Says Report', *The Guardian*, 15 October 2015.

Under Recommendations 20 and 21, member states are required to ensure that their regulated sectors:

- Identify the subject of financial transactions.
- Monitor and keep records of all financial transactions.
- Report any suspicious transactions, along with the perpetrator's identity, to national authorities.
- Share information on suspicious transactions and associated networks with the authorities.
- Collaborate with investigations.

Balancing these imperatives, the degree to which data belonging to individuals can be processed is guided by Article 8 of the European Convention on Human Rights of 1950 on the 'right to privacy and family life' and by Articles 7 and 8 of the EU Charter of Fundamental Rights on privacy and data protection.[10] These provisions are broadly intended to ensure citizens are able to safeguard personal communications and other private matters from interference by third parties. The right to privacy is, however, not absolute, and Article 8 of the EU Charter provides an exception to individual privacy in matters where a breach is necessary for 'the prevention of disorder or crime'.

The requirement to monitor transactions and report on suspicious behaviour falls under the exemptions accepted under Article 8 to share personal data for purposes of preventing and tackling crime. As noted previously, the co-existence of these frameworks appears to be provided for within both EU and UK law.

However, private sector entities – in particular financial institutions – report difficulties in implementing existing AML/CTF regulations because of jurisdictional limitations, lack of clarity of existing legislation, and the increased demand for information sharing by the FATF and national authorities responsible for disrupting crime that go beyond existing data protection laws. Similarly, public sector actors – in particular law enforcement agencies – report a significant discrepancy between the quantity of Suspicious Activity Reports (SARs) generated and the capacity to process and investigate them.

Thus the challenges are less a result of conflicting legal frameworks and more related to the specific difficulty of processing data gathered by the financial sector and shared with the authorities.

Questions are frequently raised concerning the type and uses of the data collected under the SARs regime (also referred to as the Suspicious Transaction Reporting regime). For example,

10. International agreements are normally only directed at public entities. However, their application is arguably broader, especially, as explained in this paper, given the increasing partnership between public and private sectors.

the former Article 29 Data Protection Working Party[11] – the independent advisory body on data protection at EU level – has highlighted the need for a clear distinction between the collection and processing of information for the purposes of customer due diligence and compliance with the SARs protocol.[12] Concerns have also been raised about restrictions on access to data, the correction of erroneous and inaccurate information and the use of information for purposes other than tackling money laundering and terrorist financing as envisioned in FATF's Recommendations.

Commentators and legislators emphasise the lack of clarity surrounding the purpose of data collection, how data are used, and how long they can be kept by data processors.[13] The contribution to and maintenance of the SARs regime by public and private sector actors therefore constitutes an area of potential conflict between the two frameworks that is created by the broad application of reporting by the regulated sector and the limited processing capability of the authorities in the face of ever-increasing quantities of information. This paper suggests that it is in the maintenance of the SARs database – not in the interaction between public and private actors – that some of the conflict between AML/CTF and data protection frameworks exists. It further suggests that the focus should be the quantity and relevance of data stored, how long data are retained, and the general security of the database.

Box 2: The UK SARs Regime: A Case in Point.

In the year to September 2015, the number of SARs submitted to the UK Financial Intelligence Unit (UK FIU) rose by nearly 8% to 381,882, the largest number yet received and far in excess of that envisioned for the reporting system and its database.[1] It is widely acknowledged that, although law enforcement may search the database for relevant FININT that will help build and pursue cases, it does not have the capacity to process and investigate all reports.[2] Consequently, the analysis of SARs may not go beyond an analyst's basic key-word search, identifying SARs linked to ongoing investigations.

The low threshold for report generation and the widely acknowledged practice of 'defensive reporting'[3] – the practice of precautionary reporting by the regulated sector to avoid prosecution rather than to flag a genuine suspicion – results in thousands of unnecessary SARs being filed and held in the database without being investigated or properly dismissed.

1. NCA, 'Suspicious Activity Reports (SARs) Annual Report 2015', p. 10.
2. Author interviews, August–October 2015.
3. *Ibid.*

11. With the coming into force of the EU GDPR the Article 29 Working Party will become known as the European Data Protection Board.
12. Article 29 Working Party on Data Protection 'was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'. See <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> Accessed 24 June 2016.
13. Cynthia O'Donoghue, 'Data Protection vs. Anti-Money Laundering, Counter Terrorism and Traceable Money Transfers', *Technology Law Dispatch*, 21 August 2013.

UK FIU officials argue that this material constitutes a valuable resource for informing officers about types of criminality, corroborating investigations and facilitating the identification of criminal networks, and is necessary. It acts as a useful tool 'in case we need it'.[4] However, no reasonable justification is offered for the consequences of this lack of processing capacity, or the fact that the vast majority of data will never be investigated and will, at best, be used as background information.

This paper argues that storing information on suspects for long periods without investigation does not constitute a necessary or proportionate action to combat money laundering or terrorist financing and therefore contravenes data protection principles. It maintains that the collection and retention of data relating to individuals' transactions and operations for no particular use suggests a potential contradiction with the data protection principles in that it is not 'necessary'. Evidence gathered from other EU member states' financial intelligence units and international organisations confirms that UK practice is exceptional and that, in neighbouring jurisdictions, submitted SARs (although retained for similarly long periods) are investigated and dismissed as appropriate.[5]

A further potential conflict of the UK's SARs regime with data protection concerns stems from the inadequacy of the ELMER database – the system used by the UK FIU to store SARs – to protect and process data, and its outdated software.[6] Infamous for crashing, freezing and generally malfunctioning, it fails to reassure users of its resilience.

A new database with more sophisticated search and screening capabilities would potentially reduce the number and improve the quality of SARs, through, for instance, the provision of feedback that would enable the private sector to improve the quality of its submissions.[7]

A review of the parameters of ELMER, the retention and use of data, and the obligations for compliance with data protection principles was initiated following evidence given to the House of Lords' European Union Committee by members of the Serious Organised Crime Agency (the predecessor of the current National Crime Agency, home of the UK FIU) and the Information Commissioner's Office in 2011.[8] Anecdotal evidence at that time suggested ELMER contained 1,928,677 reports, a number considered excessive and subsequently reduced to 600,000 by the end of 2011 (through deletion of obsolete files) as the Lords warned that 'if too much information is collated on low levels of suspicion the process

4. *Ibid.*
5. *Ibid.*
6. *Ibid*.
7. Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (London: The Stationery Office, 2016), p. 5. Action 1 states that the Home Office and the NCA should 'Reform the Suspicious Activity Reports (SARs) regime, making the necessary legislative, operational and technical changes to deliver the proposals detailed in the Action Plan.
8. House of Lords European Union Committee, 'Money Laundering: Data Protection for Suspicious Activity Reports', Sixth Report, 18 January 2011.

is devalued'.[9] With the adoption of the EU DPD as well as the significant increase in the number of reports being stored to the current level of approximately 2 million SARs,[10] the debate on the database's proportional and necessary nature is likely to restart. While law enforcement retains the legitimacy to create such a database, the number of records and the scale of the resources involved appear to be disproportionate to its purpose and potential benefits.

As financial crime proliferates and awareness of the utility of financial trails in tackling the problem evolves, there is an increasing need for additional information sharing between sectors.[11] For there to be improvements in the quality (and therefore the usefulness) of SARs generated by private sector entities under the AML/CTF regime, there is clearly a need for adequate feedback from the UK FIU.[12] Without this, the private sector is unable to determine which data, areas or suspicious activities are relevant to law enforcement, and therefore has no choice but to contribute to the problem of an excess of SARs identified above.

The management of the SARs regime and the obstacles to adequate data protection it creates is one of the main challenges to efficient information sharing between the private and public sectors. The system's inability to process information means that data is being shared to little purpose and not as the law intended.

9. Leo King, 'SOCA Money Laundering Database Concerns Remain, Says Lords Committee', *ComputerWorldUK*, 1 February 2011.
10. National Crime Agency, 'The SARs Regime'. Available at: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/UK FIU/the-sars-regime>, accessed 24 June 2016.
11. Clare Ellis and Inês Sofia de Oliveira, 'Tackling Money Laundering: Towards a New model for information Sharing', Conference Report, RUSI, September 2015.
12. Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance*, p. 14.

Necessity and Proportionality

The analysis above demonstrates how private-to-public information sharing for purposes of criminal investigations raises concerns about the safety, adequacy and relevance of the data collected and stored. While the UK DPA does not explicitly state the principles of 'necessity' and 'proportionality' as Article 21 of the EU GDPR does, both principles are applicable in the UK since they are derived from EU law. Once those criteria have been met, the only remaining issue is which institutions should be designated as competent authorities that are permitted to share information.

As mentioned above, current exemptions to data protection define how and when it is possible to breach aspects of individual privacy to fight crime. The GDPR states that 'Union or Member

State law may restrict [data protection] … when such a restriction constitutes a necessary and proportionate measure'.[14] The DPD elaborates on this. Consistent with this, the former Article 29 Working Party on Data Protection has stipulated that any such exemptions or restrictions should, even in the context of law enforcement, pass the test of 'necessity' and 'proportionality' through consideration of three questions:

- Is there a pressing social need?
- Is it proportionate?
- Are there relevant and sufficient reasons?[15]

As private and public bodies store increasing quantities of personal information, ensuring that data protection regimes are maintained under the right terms becomes crucial. However, the question of length of storage and use continue to pose a challenge.

Length of Storage

One of the major concerns established in the data protection debates relates to how long data should be kept to ensure that data processing is proportionate to the crime and necessary to its investigation. This is particularly pertinent to the collection and storage of SARs data within the implementation of the AML/CTF regime.

It is unclear, for example, whether storing data on individuals often based on very low suspicions, or even defensive reporting by the regulated sector, complies with these principles. Originally, SARs were kept for ten years.[16] Many feel that this appropriately reflected the time involved in the associated investigative and legal procedures, and, indeed, there are provisions to hold SARs for longer in cases of conviction – in this case outside of ELMER.[17] However, some believe that holding a suspicion on an individual for six years without apparently investigating it is excessive,[18] and this was an area of debate for the House of Lords enquiry in 2011.[19] The issue is extensively explored in the literature, with the majority of authors reporting the retention of personal (and especially sensitive) data for between one and five years.[20]

14. GDPR, Article 21.
15. Article 29 Data Protection Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection Within the Law Enforcement Sector', 536/14/EN, WP 211, 24 February 2014, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec3>, accessed 24 June 2016.
16. House of Lords European Union Committee, 'Money Laundering and the Financing of Terrorism', 19th Report of Session 2008–09, HL Paper 132–II, 22 July 2009.
17. Author interviews, August–October 2015.
18. Article 29 Data Protection Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection Within the Law Enforcement Sector'.
19. National Crime Agency, 'SARs Regime'.
20. See Information Commissioner's Office, 'Retaining Personal Data (Principle 5)', <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/>, accessed 8 July 2016; and European Commission, 'Data Retention', Migration and Home Affairs, <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/information-exchange/data-retention/index_en.htm>, accessed 8 July 2016. For a broader understanding of data protection, see Centre

The Lords' debate recommended a six-year retention timeframe based on available evidence, which included the views of the Information Commissioner's Office.[21] While this represented some progress in aligning the storage of SARs with data-protection requirements, challenges to 'necessity' and 'proportionality' remain, and research for this paper suggests that the parameters of this debate are likely to change in response to emerging case law.

Additional questions arising from the SARs structure relate to the accuracy of data held and their availability for purposes beyond those for which they were collected.

The three-question test is derived from this potential conflict of interests and a specific example of their application proves illustrative. Examining the use by UK police of the Automatic Number Plate Recognition (ANPR) system – which keeps a record of all vehicle number plates and runs them against criminal records – the former Article 29 Data Protection Working Party concluded that 'the force had failed to properly identify a sufficiently pressing social need to justify the level of intrusion into the private lives of so many (innocent) individuals'.[22] The ANPR database currently gives only some staff the right to access data for two years, with the norm being 90 days after collection.

The UK's SARs database risks being similarly condemned, especially as the formation of the Joint Money Laundering Intelligence Taskforce (JMLIT) implicitly acknowledges the desirability of an alternative system.[23]

In sum, the structure and size of the SARs regime, its inability to use the large amounts of information stored within a reasonable timeframe, and the difficulties of adequate data processing posed by outmoded software represent a challenge to the principles already discussed in this paper. Thus, while the existing information-sharing system between the private sector and UK law enforcement does not present concrete impediments to information sharing as the result of data-protection provisions, this paper suggests that a more nuanced approach is required to ensure that the principles of 'necessity' and 'proportionality' that underpin EU legislation (with their concomitant relevance to UK practice) are given thorough consideration.

---

for European Policy Studies (CEPS), 'Data and Privacy', <https://www.ceps.eu/topics/data-privacy>, accessed 26 June 2016.

21. House of Lords European Union Committee, 'Money Laundering: Data Protection for Suspicious Activity Reports'.
22. Article 29 Data Protection Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection Within the Law Enforcement Sector'.
23. Initially formed as a pilot in February 2015, the JMLIT brings together public and private sector actors under the leadership of the NCA to share and analyse information from the public and private sectors to better understand the true scale of money laundering and the methods used by criminals to exploit the UK's financial system. For more details see <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit>.

Moving Beyond the Status Quo

So, while excessive, 'defensive' reporting and the resulting size of databases may appear to challenge the principles of 'necessity' and 'proportionality', the frameworks for data protection and financial crime do not appear to conflict with one another when the *current requirements* made of public and private sector actors are considered. However, calls for greater information sharing that would go beyond the minimum mandated by the FATF raise questions as to whether the coexistence of data-protection and financial crime legislation can remain symbiotic.

The expansion of efforts to disrupt financial crime is likely to include the possibility for greater information sharing among private sector entities and the provision of greater direction by the authorities. Existing government plans, together with interviews with government officials, suggest that conflicts within the existing system are likely to arise.[24]

The Role of the Private Sector and Voluntary Information Sharing

As criminality fails to stop 'at the border', the regulated sector claims it cannot adequately tackle international crime or fulfil FATF Recommendations without expanded information-sharing capacities to include private-to-private and cross-border sharing. For example, in the UK, if a private institution submits a SAR to the FIU, it is thereafter precluded from sharing that information (the SAR and information contained therein) with other businesses and individuals – in line with 'tipping-off' provisions[25] – and is therefore prevented from assisting other businesses or jurisdictions in averting criminal activity.

Data sharing between private entities is not as clearly legally defined as that between private and public sector bodies. It is mostly guided by case law.[26] Private-to-private information sharing is not included under the existing SARs regime or the FATF Recommendations and is therefore not explicitly referred to in most national laws. Despite these legal omissions, the sharing of specific personal data between private sector entities is to some extent desirable given the monitoring and recording functions required of the private sector, as detailed below. In this regard, most would argue[27] that the absence of a legal framework for this means that DPA exemptions do not apply – with the resulting concerns about data protection.

This paper suggests that the obligation to comply with the FATF Recommendations in the context of AML/CTF generates a need to share information with actors other than the public sector for the purposes of disrupting crime effectively. It could therefore be argued that such information sharing should fall under the exemptions outlined in the new EU data protection

24. Further allowance for private-to-private information sharing is being discussed in the UK. See Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance,* para. 2.11, p. 14.
25. See FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', FATF/OECD, 2012, Recommendation 21.
26. Tournier vs. National Provincial and Union Bank of England, 17 December 1923.
27. As defended by one of the paper's peer reviewers.

package, including the DPD and GRDP. The private sector assumes an important role in the fight against financial crime, and its information-sharing activities – other than those officially required – must therefore be accounted for, with greater status, in data protection laws.

Box 3: FAQs on Private Sector Intragroup and Intergroup Information Sharing

1. Can UK Bank A share information on suspicious activity with UK Bank B (different group)?

It's complicated. There is no requirement to do so. In practice, banks are discouraged from this sort of sharing by fears of civil litigation and possible competition issues so as a consequence most claim that they are unable to share. However, a legal expert interviewed by the author (October 2015) said: 'No one will ever be prosecuted for sharing information to fight crime', a point corroborated by this paper's analysis of the private sector's 'policing function'. In practice, it is known that such sharing occasionally happens. In sum, obstacles exist but they are not data protection-related.

2. Can UK Bank A share information with German Bank A.1 (same group) regarding a SAR that concerns both?

Yes. While not overtly defined in domestic law, Article 39 of the EU Fourth AML Directive (to be implemented as soon as possible by EU member states) explicitly states that the prohibition to disclose the existence of an investigation should not affect sharing within the same group, provided the same safeguards are applied. This provision could additionally be safeguarded by the fact that most banks include a consent clause for this in their terms and conditions.

3. Can UK Bank A share information with US Bank C?

No. Unless Bank C is based in a country which upholds equal data-protection provisions as those practised in the EU (normally determined by national legislation).

In this sense, the sharing of information between private sector entities, though voluntary, is arguably still meeting the requirements of the AML/CTF framework. Private entities have rights over personal data as long as it is processed in accordance with data protection principles, existing DPA exemptions and/or the consent of the individual concerned. A brief comparative analysis of the terms and conditions of a number of financial institutions demonstrates that most already include 'consent' provisions for sharing within companies in the same commercial group and with third parties for purposes of tackling crime (see Annex 1). This corroborates the suspicion that, if financial institutions fail to act on these provisions, it is due to uncertainty about the precise legal implications of sharing within the EU, as well as concerns about commercial competitive advantage.

The literature argues that the lack of resources identified as being a problem in most law enforcement bodies has put the private sector at the forefront of information collection,

investigation and even self-monitoring. Michael Levi highlights how partnerships in fighting crime are becoming more widespread, citing the area of fraud and coining the term 'policing beyond the police'.[28] This paper agrees, given the provisions of the FATF Recommendations, subsequent practice and the obligation to monitor, record and report.

Similarly, in the recent EU GDPR and DPD negotiations between the EU Parliament, Commission and Council, the UK suggested amending the wording of the DPD to add that 'such competent authorities may include not only public authorities such as the judicial authorities, the police or other law enforcement authorities but also any body/entity entrusted by national law to performing [sic] public duties or exercising public powers'.[29] Although it was unsuccessful, there is a growing recognition that, while under the EU GDPR the private sector may share information under supervision or as authorised, there is also a need for voluntary information sharing between private actors to be included in the DPD and its specific focus on law enforcement and crime prevention actions.

This paper's analysis of the challenges involved in information sharing is predicated on the assumption that the private sector is increasingly carrying out 'police-like' functions and that laws should be amended to reflect this or risk being incomplete.

The author of this paper argues that the challenges posed by current provisions for the voluntary sharing of information between private sector actors are already being addressed by the new EU Fourth AML Directive. In particular, the directive addresses issues relating to intragroup sharing for the purposes of disrupting crime and safeguarding public security within national borders, provided consent is obtained, for instance in the business terms and conditions.[30]

It is expected that the implementation of the EU Fourth AML Directive in the UK – intended to be concluded by the end of 2016[31] – will confirm and clarify intra-group information-sharing practice that is already tacitly accepted.[32] Similarly, exemptions from inter-group EU cross-border information sharing may also be tacitly accepted, given that the DPA stipulates

28. Michael Levi, 'Public and Private Policing of Financial Crimes: The Struggle for Co-Ordination', *Journal of Criminal Justice and Security* (Vol. 12, No. 4, 2010), pp. 343–54.
29. Statewatch, 'EU Bookmark and Share DATA PROTECTION REGULATION: Council of the European Union: LIMITE documents 26.5.15', 20 May 2015, <http://statewatch.org/news/2015/may/eu-dp-reg-may-2015.htm>, accessed 27 June 2016. Under the EU data protection package (especially the DPD), information may be shared only to 'competent authorities', to include public but not private organisations. See European Commission, 'Proposal for a Directive of the European Parliament and of the Council 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'.
30. This paper's focus is on data protection and therefore any commercial or competition-related impediments to information sharing are outside its scope.
31. Michael McKee, Tony Katz, Ian Mason and Sam Millar, 'EU Action Plan on Strengthening the Fight Against Terrorist Financing and Tightening Deadline of MLD4 Implementation', *Lexology*, 11 April 2016, <http://www.lexology.com/library/detail.aspx?g=597a24e5-3108-4888-b2fb-c2a69e9204b1>, accessed 8 July 2016.
32. Author interview with EU Commission personnel, October 2015.

nothing to the contrary and that AML/CTF requirements call for it. Article 39 Section 4 of the Fourth AML Directive states that the prohibition to inform an individual of data collection or an ongoing investigation 'shall not prevent disclosure between institutions from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive provided that they belong to the same group'. The accommodation for the sharing of data between EU member states is thus based on assurances of the existence of equivalent data protection standards, which the EU GDPR supplies. The inference to be drawn from this assumption, therefore, is that there are no legal restrictions on parties involved in inter-group cross-border data sharing within the Union.

While steps are being taken to explicitly recognise the private sector's 'policing function', challenges remain, including fear of civil litigation, competition and corporate secrecy and, in some cases, the realisation that data do not stop at the EU border.

Based on this analysis, the Q&A presented in Box 3 clarifies the situation for the private sector regarding the upcoming data protection and AML regulations.

A universal voluntary information-sharing framework that allows the private sector more powers and to share as needed would enhance the effectiveness of efforts to disrupt crime. However, by definition, data-protection provisions would always seek to limit the application of such additional flexibility to comparable jurisdictions with equivalent standards. There would still be considerable obstacles to the sharing of information for AML/CTF purposes with jurisdictions (for example, outside the EU) whose data-protection provisions are deemed inadequate.

As mentioned above, the civil and criminal litigation costs of sharing in the absence of EU-required safeguards could be significant. In light of this, despite the private sector's requests for increased information-sharing powers and the recognition that these might be needed, a viable instrument to allow for global information sharing could prove difficult to construct.

Although within the EU, voluntary information sharing between private sector entities could easily be made a reality in the near future, the topic will remain controversial for three reasons: first, the exemption to the safeguards of individual rights exists *de jure* only for state parties, law enforcement and intelligence services, and then only for the purposes of investigating crime. Second, the tacit extension of the legal framework on information sharing to encompass the private sector – in recognition of the fact that it is a de facto 'policing' force – is only now becoming codified and still receives limited official recognition. Third, the private sector has come to play such a vital function in the disruption of crime that, if it continues to do so without the appropriate legal implements at its disposal, data sharing, even for purposes of criminal investigations, will be severely restricted. The initial spirit of the DPA and the AML/CTF frameworks defined law enforcement and government agencies alone as the 'competent authorities' for performing crime-disrupting functions.[33] The rapidly expanding

33. Competent authorities 'means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'. See European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the

partnership with the private sector for purposes of disrupting crime has evolved beyond the remit contained in the original legislation and its impact at all levels is still to be assessed.

Despite some suspension of the right to privacy for the subject of an investigation – as defined above – the 'social contract' between the state and the individual establishes an expectation of responsibility and accountability that does not exist in the relationship between a financial institution and an individual. The same concept should be incorporated into any normalisation of private-to-private sector information sharing to ensure accountability and transparency in data processing. Interviews conducted during research for this paper confirmed that it is the prospect of prosecution for mishandling data, and fears of competition, that impede information sharing between private sector actors.[34] Having appropriate individual data protection systems in place would help mitigate these concerns. The results of information sharing between financial institutions can include 'de-banking' – the closure of accounts and financial exclusion for suspects of criminal activity as well as the challenges of competition law where there is a concerted action to de-risk. Financial institutions are under no obligation to offer financial services to persons deemed high-risk (in terms of their financial stability or potential criminal links). For example, if an individual were the subject of three SARs, their bank might terminate the service it provided without needing to justify the decision.[35] The use and sharing of suspicious activity information may increase the likelihood that:

- Individuals are cut off from accessing financial services and forced to find alternative means of accessing and moving capital.
- Individuals see information on their financial activity shared with multiple actors and lose access and control of the veracity of data shared.

Such outcomes would constitute a violation of the principle of 'proportionality' as well as the unlawful processing of data, as de-banking does not, per se, contribute to the disruption of crime, but denies financial access to those legitimately deserving of it or drives criminal activity into unregulated systems inaccessible to monitoring by law enforcement.

Some of these fears may be well founded and certainly warrant further consideration. The table in Annex 1 demonstrates the frequent ambiguity of financial institutions' terms and conditions, and their different practices and interpretations of the law. Standardisation would help bring clarity to the processing of data and a greater understanding of its implications.

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', Article 3.

34. Author interviews conducted in August, September and October 2015.
35. *Ibid*. Note that de-banking practices are private and carried out differently within each organisation. It is not possible for the regulator to ensure that an individual is not de-banked as a consequence of SARs filings, even if guilt is unproven. Due to tipping-off provisions contained in Section 7 of the Proceeds of Crime Act 2002), individuals are also unable to establish whether a SAR is behind the reason for de-banking.

In sum, this paper suggests that information-sharing challenges faced by the private sector are inextricably linked to the restrictions and problems brought about by the SARs regime and an outmoded and restrictive interpretation of what constitute *competent* authorities – or actors mandated by authorities – in the sphere of voluntary information sharing.

Conclusion

This paper's analysis of the challenges posed to AML/CTF by data protection suggests there is no conflict between the two frameworks as they are intended to operate today. Furthermore, it argues that the ambition of the private sector to share beyond what existing provisions allow – further to the responsibilities it has been awarded by the FATF – cannot be considered in conflict with current regulation because this ambition, in effect, demands a new regulatory framework that reflects changing current concerns and expanded objectives. Difficulties with the current regime stem – particularly in the UK – primarily from the vast amount of data retained by the authorities 'just in case', which then undergo little scrutiny.

The data-protection regime's critical deficiency lies in its failure to recognise the demands made on the private sector by authorities which seek to co-opt banks and other regulated entities to assist with the fight against financial crime and terrorist finance, but which simultaneously limit their ability to share information beyond the parameters laid out by existing legislation. Broadly, it is suggested that the increasing need for information sharing between different actors and across borders demands:

1. Reform of the SARs regime to provide greater flexibility for information to be shared.
2. Revision of the concept of 'competent authorities' to include the private sector – or to ensure it is specifically mandated to share information – which will lead to the creation of better quality SARs and more effective risk mitigation.

This paper suggests that current AML/CTF and data-protection frameworks can co-exist, but risk growing deficiencies in implementation and results if the role of the private sector remains unacknowledged by the provisions of relevant laws. It further suggests that, while changes to regulations are desirable, it is important to uphold the principles of 'necessity' and 'proportionality' – and ensure adoption by the private sector – to maintain individual rights and the important balance between privacy and security.

Recommendations

This paper offers five recommendations to ensure that the greater information sharing called for by global leaders is developed in a manner consistent with the concepts of 'necessity' and 'proportionality', balancing a heightened focus on security with continued data protection and privacy.

1. Current regulations need to be clarified and supplemented with guidance that removes concerns (primarily of interpretation) so that information sharing is maximised under

the existing frameworks. EU-level and national authorities (for example, led by the Information Commissioner's Office in the UK) should call for identified barriers to be reported so that they can be assessed and addressed or dismissed.

2. State authorities should provide better guidance to their regulated sectors so that the excessive amount of data submitted by them and held by law enforcement can be reduced in line with the concepts of 'necessity' and 'proportionality'. In particular, this means that enhancements to the databases used by law enforcement for receiving and analysing SARs should be implemented so that reports submitted by the private sector can be rapidly and effectively exploited, providing feedback that will lead to fewer and better submissions. The setting up in 2015 of the UK's innovative information-sharing system, the JMLIT, is a welcome step in this regard.
3. Legal authorisation should be given to facilitate private-to-private information sharing and allow the private sector to work together to enhance the quality of reporting so that reported information is confined to genuine cases of financial crime concern. EU member states should promote provisions under which EU-based private sector actors may share and process data voluntarily for purposes of crime prevention. EU-wide guidance should be agreed, produced and disseminated.
4. While data protection exemptions are bestowed upon law enforcement, despite the financial crime *policing* responsibility placed on the private sector, an inequality of treatment means that it needs to be supervised or authorised by governments or EU law to share information. Thus, as the expectation on the sector to play a significant role in disrupting financial crime grows, consideration should be given to developing the framework within which it operates in this field to include relevant private sector-led activity akin to that awarded to law enforcement and other authorities.
5. To countermand concerns that data held by the private sector is too easily available to security authorities or other private sector actors, the private sector should revise data-protection policies and provide sufficient assurance that information collected to tackle financial crime is not used for any other purposes. Standardisation across institutions in this area would be a useful step towards greater clarity and the protection of citizen rights. Furthermore, information shared within EU jurisdictions must allow for amendment, updating and deletion when fairly required by the data subject or authorities.

Annex 1: Data Sharing Terms

Figure 1: Terms and Conditions Compared under which Information May be Collected, Shared and Processed

Institution	Data Sharing within Group	Data Sharing with others	Data Processing
RBS[1]	For varied purposes including to 'prevent and detect crime, including fraud and money laundering'	'Where permitted by law, it is necessary for our legitimate interests or those of a third party, and it is not inconsistent with the purposes listed above'. RBS will transfer customer information to organisations in other countries provided that they protect it 'in the same way we would and in accordance with applicable laws'	Standard business practice clearly defined in 1.5 of Terms and Conditions
Nationwide[2]	'Any information about me and my account may be shared within Nationwide to open and manage the account, make lending decisions, collect debts, trace debtors, prevent fraud and money laundering and for business analysis'	'It may also be shared with other organisations for the purposes of them providing products and services in association with or on behalf of Nationwide'	'May pass information to financial and other organisations involved in fraud prevention to protect yourselves and your customers from theft and fraud. If I give you false or inaccurate information and you identify fraud, you will record this and pass it to fraud prevention agencies to prevent fraud and money laundering'
Citibank[3]	'For crime and fraud prevention, and debt recovery (including tracing you if we do not have up-to-date details)'	'We will also disclose your information: a) to our insurers, sub-contractors and persons acting as our agents who have agreed to keep your information strictly confidential; (b) to linked suppliers to the extent that they need your information to provide additional benefits or services to you; (c) To any bank, financial institution or company to whom we may assign or transfer our rights and/or duties under this Agreement; or (d) If we are required or permitted to do so by Applicable Law, including to Authorities'	'So that we can provide products and services designed especially for you, we will collect and review all the Information'

Institution	Data Sharing within Group	Data Sharing with Others	Data Processing
Lloyds[4]	'We may share the personal information we hold about you across the Lloyds Banking Group … crime detection, prevention, and prosecution; … we may need to disclose information to government bodies'	'We may share it with each other and disclose it outside the Lloyds Banking Group if: … required by us or others to investigate or prevent crime'	'Personal information will be shared within the Lloyds Banking Group so that we and any other companies in our Group can look after your relationship with us'
HSBC[5]	'To any member of the HSBC Group and anybody who provides services to them or their agents'	Third parties 'may also use, transfer and disclose Customer Information for the same purposes, and they may be in countries where data protection laws don't provide the same level of protection as in the UK. However, whether it is processed in the UK or overseas, Customer Information will be protected by a strict code of secrecy and security which all members of the HSBC Group, their staff and third parties are subject to'	'Meet Compliance Obligations … for the internal operational requirements for members of the HSBC Group (including, for example, product development, insurance, audit and credit and risk management)'
Santander[6]	'We may share your information as explained in this statement with the group of companies to which we belong (the Santander group) and our associated companies and with people who are acting on our behalf'	'You understand that we will make sure your information is only used in line with our instructions and will be kept safe. If we transfer your information to another country, we will also make sure it is protected, as it would be under the UK Data Protection Act'	'We may use all the information you give to us or we hold on you to run the account(s) or service(s) and for administration purposes'

1. RBS, 'Current Accounts and Savings Terms and Conditions', <http://personal.rbs.co.uk/personal/current-accounts/terms-and conditions.html>, accessed 8 July 2016.
2. Nationwide, 'Your Current Account Terms', <http://www.nationwide.co.uk/~/media/MainSite/documents/products/current-accounts/shared/P857_ImportantInformation-TermsAndConditions.pdf>, accessed 8 July 2016.
3. Citi Bank, 'General Terms and Conditions for Citi Current Accounts and Savings Accounts', <https://www.citibank.co.uk/personal/documents.do?name=terms>, accessed 8 July 2016.
4. Lloyds Bank, 'Privacy', <http://www.lloydsbank.com/privacy.asp#collapse3-1424165610473>, accessed 8 July 2016.
5. HSBC, 'General Terms and Conditions', <http://www.hsbc.co.uk/1/PA_esf-ca-app-content/content/pws/content/personal/pdfs/general-tcs.pdf>, accessed 8 July 2016.
6. Santander, '123 Current Account Terms and Conditions', <http://www.santander.co.uk/uk/current-accounts/123-current-account-terms-and-conditions-pre-apply>, accessed 8 July 2016.

About the Author

Inês Sofia de Oliveira is a Research Fellow within the Centre for Financial Crime and Security Studies at RUSI, where she leads projects on illicit financial flows and works on projects aimed at improving public–private partnerships and information sharing. Her current research includes the 'Cartography of Compliance', a project that identifies, describes and analyses different compliance strategies adopted by the private sector in order to comply with regulatory requirements.