SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2014-008

MULTINATIONAL BANKING AND CONFLICTS AMONG US-EU AML/CTF COMPLIANCE & PRIVACY LAW: OPERATIONAL & POLITICAL VIEWS IN CONTEXT

DR. MICHELLE FRASHER

PUBLICATION DATE: 1 JULY 2016

Multinational Banking and Conflicts among US-EU AML/CTF Compliance & Privacy Law: Operational & Political Views in Context

Dr. Michelle Frasher, Ph.D.[*] with Brian Agnew, MPP[†]

Abstract:

In Information Statecraft, states employ legal and technological methods to acquire data to map behaviors and expose the illicit economy and networks of political violence. Yet, because financial institutions (FIs) possess that data, governments must depend on their cooperation. Financial data is both commercial and a source of intelligence and is governed by two often opposing legal regimes.

A comparative analysis of US and EU AML/CTF and data protection laws illuminated issues within 19 compliance areas that will challenge multinationals as they integrate privacy into AML/CTF operations. The EU's 4th Anti-Money Laundering Directive (4AMLD) promotes enterprise-wide compliance programs with data protection across the group, and US law restricts data due to confidentiality concerns and does not require privacy in compliance programs, which created risks at every point in the study. Other areas of high regulatory (and reputational) risk for multinational financial institutions lay in local authority data requests; sensitive data collection and transfers involving politically exposed persons and their families; vendor compliance with the US-EU Privacy Shield; the prohibition of KYC data use for commercial purposes for EU data subjects; and the practice of profiling and monitoring client relationships using semi-automated and automated software. Profiling deserves special attention since the EU General Data Protection Regulation (GDPR) gives data subjects the right to object to profiling, to understand the legal outcomes of computer-aided decision-making, and the right to challenge these decisions (applicable to de-risking), but with restrictions according to Member State law.

Data privacy programs benefit AML/CTF compliance because they create accountability trails, help FIs produce better data to authorities, and lend reputational currency. Despite the regulatory conflicts, the financial services have an opportunity to contribute to data privacy/AML/CTF solutions that fit their operations as the GDPR invites private associations to create codes of conduct. The private sector should develop these codes in tandem and in cooperation with Member State efforts to create technological and operational data safeguards that will be written in the next two years. Firms should prepare for these changes by conducting data inventories, mapping data flows, creating integrated AML/CTF, information technology, and privacy compliance teams, or incentivizing cross-disciplinary training for their employees so they can implement multidisciplinary and trans-jurisdictional policies and procedures.

[*] Corresponding author. mfrasher@frasher.cc Dr. Frasher wishes to thank the European Union Center, University of Illinois at Urbana-Champaign, where she was a non-resident Research Scholar for the majority of this research. Thanks to the SWIFT Institute for funding support. Professor Marieke de Goede (University of Amsterdam), Alex Zerden, Alaina Gimbert, and Dave van Moppes (Tuerlinckx Fiscale Advocaten, Belgium) contributed much-appreciated comments to early drafts. Special thanks goes to the Association of Certified Anti-Money Specialists (ACAMS), Association of Certified Financial Crimes Specialists (ACFCS), the International Association of Privacy Professionals (IAPP), for invitations to speak and interact with their members. Finally, thanks to those in the transatlantic financial services community who generously provided their time and expertise. All interviews given on condition of anonymity. This work was not influenced in any way by members of the financial services or SWIFT. All errors are my own.

[†] Brian Agnew, MPP b.d.agnew@gmail.com contributed to research, editing, and data visualizations.

TABLE OF CONTENTS

1. **INFORMATION STATECRAFT**

Information Statecraft[1] - the attempt to influence, through law and technology, the acquisition, control, or presentation of data, information, or knowledge – empowers governments to extend their political, social, security, and cultural policies across issues and borders. Financial data is of special interest to states as it can help track illicit economic flows and networks of political violence.

However, the borderless nature of financial data means that its *ownership* changes according to national views of privacy, which affects the state's ability to access it and use it. And as private companies hold much of the data that states desire, governments need the cooperation of financial institutions to acquire it. The financial system's global reach makes financial data a valuable power resource.

For financial institutions (FI), this data helps create business strategies, empowers trading capacity, protects banks from predatory competitors and bank runs, determines client and market behaviors, can produce profits if used effectively, and has even been monetized itself. The industry is bound to sovereign laws, so it must provide data to law enforcement or regulatory authorities, but due to a lack of standardization in regulations and reporting methods banks still have a lot of control over what they report.

Thus, financial data exists in a duality – it is both commercial and a source of actionable intelligence for governments.[a] Anti-Money Laundering (AML) and Counter-Terrorism Finance (CTF) presents a conundrum for states and market actors alike because the duality of financial data means that it is governed by two sometimes opposing regimes: AML and CTF laws that seek to protect the financial system from fraud, crime, and political violence; and data protection and privacy laws that seek to protect an individual's identity and choices from government and private abuse. Hence, a study of data protection or privacy law is essential to understand data control and use. National differences among these laws and their conflict with AML/CTF requirements can create serious issues for states trying to acquire financial intelligence, and for the multinational financial institutions (MFIs) expected to provide it.

[a] This paper is part of a manuscript project entitled *Information Statecraft: States, Financial Institutions, Individuals and the Politics of Counter-Terrorism Data*. Information Statecraft is not limited to the financial sector. All data exists in this duality as it can be used beyond its initial purpose. I will address technology in subsequent works.

1.1: Structure of Research

While Information Statecraft is applicable to all types of information since all data can be analyzed and used beyond its primary intent, this research set out to examine financial data's role in US and EU attempts to combat the illicit economy and political violence, and how privacy law affects those efforts. It quickly became apparent that the financial services have actively implemented AML/CTF requirements, but they have just begun to approach integrating data privacy into these operations due to the uncertainties of a newly evolving legal landscape. In fact, only in the past year has EU-driven legislation emerged, specifically within the Fourth Anti-Money Laundering Directive (4AMLD) and the General Data Protection Regulation (GDPR), that commit multinational companies to these practices in their operations across the globe. This analysis assesses the potential issues the financial services will encounter as they try to comply with (often) contrasting regulatory requirements.

The study chose 19 AML/CTF compliance areas from the Financial Action Task Force's (FATF) 49 Recommendations and then compared US *federal* and *EU-level* AML/CTF laws with federal and regional data privacy laws,[b] and calculated how inconsistencies among them may affect implementing data protection and privacy into AML/CTF compliance.[c] Theoretically, the empirical study shows how Information Statecraft contributes to international relations theory by illustrating the *interactions* and *interdependencies* among governments and financial institutions in the pursuit of the illicit economy and political violence. Narrowly, the analysis demonstrates how dissimilar data privacy regimes in the US and EU, and conflicts among AML/CTF requirements, create regulatory risks for the financial services, and how this may undercut authorities' abilities to gather actionable intelligence.

The demands of this topic exceed the aims of one paper, and as this exercise is intended for a larger volume on the subject, some clarifications are in order.

[b] See bibliography. US State and EU Member State laws sometimes provided to illustrate legislative complexity.

[c] The author conducted 30 formal interviews in the US and Europe in 2015 as a Fulbright-Schuman Scholar, and in 2015-16 under the support of the SWIFT Institute grant. Additional insights gathered through participation in AML and privacy conferences, and via email and verbal contact with members of IAPP, ACAMS, and ACFCS. Due to the sensitive nature of the topic, all interviews were given on condition of anonymity and only cited when not quoted.

This paper **does not**,

1) represent a comprehensive analysis of the AML/CTF and privacy issues or players. For example, it does not discuss data transfers between authorities or international organizations; sanctions, virtual currencies, information security, encryption; or designated non-financial businesses and professions (DNFBPs), Money Services Businesses (MSB), and non-profit organizations (NPOs).

This paper **does**,

1) use the term financial institutions (FIs) to reference multinational banks and depository institutions as they handle natural person's data and are therefore most susceptible to data protection regulation in AML/CTF;
2) target AML/CTF compliance professionals, but provides an overview of transatlantic privacy laws to inform knowledge gaps;
3) present a comparative transatlantic legal analysis of 19 privacy and AML/CTF issues to highlight conflicts that will challenge implementing data privacy into AML/CTF practices that will affect government attempts to gather data and employ Information Statecraft.

2. PRIVACY LAW & FINANCE

2.1: Data Protection/Privacy/Data Privacy

To understand how MFIs collect data and why this data is important to states to track illicit flows, one must examine data governance through privacy laws and regulations, which are the strongest state determinants of data ownership. Privacy and data protection are used interchangeably throughout this text, but their meanings change depending on the geographical and cultural locations. In the transatlantic context Europeans typically speak of privacy as an individual's human right or social condition with data protection acting as its legal safeguard. For the US, data protection and privacy are used reciprocally.

The regulation of trans-border data flows seeks to: make sure the private and public sectors do not circumvent national laws, guard against risk for data managed in other states, implement rights abroad and lastly create or maintain individual or consumer trust.[2] The globalization of the world economy, encouraged by corporate and government actors, has contributed to a web of

interests and laws that have shaped the national and transnational governance of financial data, which has not made these aims easy to achieve.

This work focuses on the commercial private sector, and analyses intergovernmental data transfers as they affect FIs. Therefore, the reader should understand the organization of privacy laws, which target certain actors and certain types of data.[3] For example, EU 95/46/EC and now the General Data Protection Regulation (COM/2012/0011 or GDPR) regulates commercial data transfers - private entity to private entity. Once that data was delivered to state or supervisory authorities, applicable laws change. EU Council Framework Decision 2008/977/JHA governs cross-border data transfers among Member State authorities, but it does not apply to private companies. In the US, the Privacy Act of 1974 governs access to individual's personally identifiable information held in federal records, and under the Freedom of Information Act (FOIA) individuals can petition for disclosure of executive branch records, regardless of citizenship. Neither apply to records held by private companies, but controversies surrounding these laws may still affect FIs.

2.2: Financial Privacy in the EU

In the EU, data ownership is vested to the individual, no matter what entity - government, another person, bank, etc. - possesses that data. Although there are exceptions, European law upholds the right of the individual to consent to its collection and usage. As a result, Europe has some of the most comprehensive rules-based data protection laws in the world, with an eye to technologies that have made it easier to spread information, and harder for individuals to maintain their control over it.

Europe has a long history of anchoring privacy to the individual.[4] Data regulation originated in France and Germany to protect the dignity of the nobility from media intrusions. Germans were the first to codify these principles as the right to personality, or *Personlichkeit*, and link individual liberty and freedom to information self-determination, or the right to control and create one's image in society.[5] After the Second World War, *Personlichkeit* became ingrained in Europe's privacy ethos.[6] The 1950 European Convention on Human Rights (ECHR) defined the parameters of privacy in "family life" "home" and "correspondence" and noted exemptions- "…in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

During the 1960s, governments, telecommunications providers, and banks began to collect, transfer, and store large amounts of data so some European states enacted legislation for health, education, and benefits information.[7] The asymmetrical legal coverage prompted steps towards regional harmonization and in 1981 the Council of Europe (CoE) Convention 108 adopted the Organization for Economic Cooperation and Development's (OECD) 1980 recommendations to standardize the collection and processing of data with a focus on automation, storage, accuracy, confidentiality, and disclosure from both private and public sources.

European states were slow to adopt these principles, which necessitated Directive 95/46/EC that applied "to data processed by automated means and data contained in or intended to be part of non-automated filing systems." For the most part of the Directive's life, AML/CTF has been included in derogations for the processing of data in the "public interest." [8] In December 2015, the EU agreed to the GDPR[d] which replaces 95/46/EC and aims to eliminate Member State differences and harmonize privacy law across Europe. The Regulation preserves the legality of processing in the public interest, but it does not fully exempt AML/CTF and requires Member States to enact certain safeguards in these circumstances. Data protection's inclusion in the 2015 4th Money Laundering Directive (4AMLD) means that the financial services can no longer rely on these exceptions.

95/46/EC's transformation to a Regulation was partially motivated by its confinement to the governance of commercial data. When the 95/46/EC was enacted under the Maastricht Treaty, European integration was organized into three legal Pillars; I) economic, social, cultural, immigration and borders; II) common foreign policy and security; and III) police and judicial cooperation in criminal matters. 95/46/EC fell under Pillar I to protect individuals from private intrusions, but did not cover data involved in national security and criminal proceedings. In 2009, the Lisbon Treaty abolished the Pillar system and the EU has been working to eliminate these derogations and apply standardized data protection rules across issue areas.

For years, EU law, and multinationals, have struggled with the duality of financial data that meant abiding by Pillar I privacy protections, but existing under a separate legal regime where their data was of interest in Pillar II and III operations like AML/CTF. The inclusion of data protection into 4AMLD is part of the Lisbon's reconciliation process. The GDPR attempts to remove intra-European discrepancies and strengthen and deepen its reach in criminal and judicial matters, including AML/CTF. Recital 40 seems to acknowledge financial data's operational duality by recognizing that data collected for commercial use can be further legally processed for related purposes like AML/CTF.

[d] The following citations refer to the GDPR as of 15 December 2015. The final articles and wording may change.

> Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller.

This does not help FIs identify their data protection duties within AML/CTF operations, but the EU's attempts to harmonize data protection law may make it easier for firms to establish group-wide rules that will lower the cost of implementing 4AMLD's privacy requirements.[9]

2.2a: Controllers, Processors & Technical and Organizational Measures

The legal analysis below places 95/46/EC and the GDPR in the context of specific compliance issues, but it is helpful to understand some of the basic terminologies components of EU privacy law.[10] Chart 1 summarizes areas not covered in this narrative, but may affect MFIs.

EU law does not distinguish between the citizenship of the data subject and the origin of the data – European protections govern the data *wherever it may be located*.[11] Unlike the 95/46/EC, where controllers were solely held accountable, the GDPR holds both controllers and processors liable for data processing. A data controller is "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." The Regulation introduces joint controllers where several entities determine the means and purposes of processing.[12] Processors are "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."[13] Controllers and processors must implement "appropriate technical and organizational measures to ensure and be able to demonstrate" compliance with the Regulation for any service they perform.[14] In MFI environments, many companies manage employees and customer databases within central systems. Parent companies (either in or outside of the EU) must clearly define their subsidiary and affiliate data relationships and the extent to which the parent company or the local entity determines the means and purpose of their data processing.

The phrase technical and organizational measures is used throughout the text[15] and the GDPR invites the development of industry best practices or "codes of conduct" so controllers and processors can prove compliance. The Regulation allows the European Data Protection Board (EDPB) and Commission to create codes, and the GDPR specifically encourages "associations and other bodies" of controllers to "amend or extend" these codes. After approval by supervisory

authorities of the Member State of main establishment (central authority), the EDPB, the Commission, make the codes public.[16] Here, the financial services may find a way forward for best practices to solve many of the AML/CTF and privacy conflicts in Section 3.

Processing is lawful when data subjects give their "freely given, specific, informed and unambiguous" consent; when necessary in the course of establishing a business relationship; in accordance to a legal obligation; to protect the vital interests of the subject; or the public interest and "legitimate interests" of the controller.[17] Data should only be collected for explicit and legitimate purposes, adequate and relative purposes, kept up-to-date, and with security measures (as appropriate) such as encryption and privacy enabled technologies.[18]

Table 1: The General Data Protection Regulation & Issues for MFIs

Personal data (PII)	"any information relating to an identified or identifiable natural person 'data subject…who can be identified, directly or indirectly. (Art. 4) Includes location data and on-line identifiers, such as IP addresses.
Consent	"freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed" (Art. 4) Controller and processor bear burden of proof.
Sensitive Data	Consent must be "explicit." Only processed under the control of official authority or when authorised by Union law or Member State law that provides adequate safeguards for the rights and freedoms of data subjects. (Art. 9(a))
Establishment	Firms with more than one location can designate a "main establishment" where central administration (or other) makes the decisions as to the purposes of processing. Location determines lead supervisory authority. Processor main establishment will be its administrative center. Controllers outside EU must appoint a representative to act on behalf of controller and interact with supervisory authorities. (Art. 25)
Lead Authority	Firms that have multiple establishments will have a single SA in main establishment Member State that will act as a "One Stop Shop" to supervise processing in EU. (Rec. 97)
Data Protection Officer	Required when operations require "regular and systematic monitoring of data subjects on a large scale." A group may appoint one DPO if they are accessible to each establishment. Can be a member of firm already as long as other duties do not conflict. (Art. 35 & Art. 36 for duties)
Data Protection Impact Assessment	Obligatory (under mandate from supervising authority) for profiling and automated processing operations, criminal conviction data, when not required under another law (Art. 33).
Privacy by Default/ Design	Implement mechanisms so personal data is processed only for intended purposes. Must build privacy into new technologies, products, and services. (Recs. 61, 83, Arts. 23, 43)

Enforcement & Consistency Mechanism	Creation of European Data Protection Board (EDPB). (Art. 64) Member States determine procedures for National Supervisory Authorities (SAs) SAs can force controllers or processors to provide information and ban processing. SAs will consult with other affected SAs and in some cases the EDPB. Includes: multi-jurisdictional enforcement; BCRs, Model Clauses, Codes of Conduct (Art. 38) and Certification (Art. 39). (Arts. 46, 47, 48, 49, 51, 51(a), 52, 53)
Data Subject Redress & Compensation	Data subjects can sue SAs to act on complaints. (Art. 73) Firms, individuals can appeal SA actions in national courts. (Art. 74). Right to remedy against controller or processor and obtain compensation for damage suffered (Art. 75, 76, 77).
Penalties & Fines	Fines "effective, proportionate and dissuasive" to the discretion of SAs (Denmark and Estonia excepted). Depending on offense, administrative fines to 10,000,000 € or 2% of total worldwide annual turnover or to 20,000,000 € or 4% of total worldwide annual turnover, whichever is higher. (Art. 79) Fines on individuals taking into account "general level of income" (Rec. 120)

2.2b: Exceptions & Data Transfers: Binding Corporate Rules & Model Clauses

Like 95/46/EC, the GDPR authorizes the European Commission to determine if a third country provides an "adequate" level of data privacy protections for transfers of EU data.[19] In cases without an adequacy Decision, the GDPR carries over 95/46/EC's exemptions for Member States to restrict "obligations and rights" when data processing pertained to national security, defence, public security, criminal investigations, economic or financial interests, and regulatory duties related to these issues, which includes AML/CTF.[20] Unlike the Directive, the Regulation requires "any legislative measure" that deals with this data to include "specific provisions at least, where relevant" that outline the purposes and categories of processing and type of data, scope of restrictions, safeguards for unlawful transfers, storage periods, risks to rights and freedoms and that data subjects be informed of the restrictions.[21] Member States will likely interpret and enforce these exceptions and their safeguards differently.

GDPR Article 44 states that even without an adequacy Decision or appropriate safeguards, Member States can allow transfers to third countries or international organizations when a data subject has consented and been informed of the risks, when necessary for the performance or conclusion of a contract, and for reasons of public interest.[22] Article 44(h)[23] does not permit bulk transfers for commercial or marketing purposes, but authorizes bulk flows for AML/CTF compliance [emphasis added];

> Where a transfer could not be based on a provision in Articles 41 [Adequacy Decision] or 42 [Appropriate Safeguards], including binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) is applicable [the reasons listed above], a transfer to a third country or an international organisation may take place only if the transfer is *not repetitive, concerns only a limited number of data subjects*, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not

> overridden by the interests or rights and freedoms of the data subject, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data…

Article 44 appears to omit AML/CTF compliance from data protection, but this view is superficial. In their review of 4AMLD, data protection authorities believe exceptions should be applied *narrowly* and should not pertain to the large and regular data transfers that are the reality of the financial system or AML compliance. While the GDPR may shield intra-firm bulk transfers when carried out for AML/CTF purposes, the Regulation stipulates that Member States set "suitable safeguards" when doing so. Both the Regulation and 4AMLD allocate the power to limit transfers and set safeguards, and the GDPR does offer a broad outline about how technical and organizational safeguards should be applied in these cases.

The commercial and potentially criminal duality of financial data also creates difficulties for relying on the Article 44 exception. Although compliance teams will breathe easier knowing they can share data among the group (See Section 3.10) to carry out their duties, it is less clear when the commercial nature of financial data begins and ends, and thus where the exception begins, and ends. In 2013, the EDPS recognized this problem noting that ""…the collection of data for anti-money laundering purposes takes place at the same time as the collection of data for commercial purposes."

Where data must be transferred to states without an adequacy decision, the Regulation retains Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs), also known as Model Clauses. BCRs or SCCs already in place will be honored after the GDPR goes into effect, but subject to "on-going" review.[24]

BCRs are internal and legally binding rules of conduct for multinational companies (controllers and processors) [25] that have entities located in states that do not have adequate level of privacy protections. They have been one of the few legal avenues for US-EU private data transfers within a group. Under 95/46/EC, BCR requirements were set by Working Party 29 (WP29)[e] standards, but the Regulation now enumerates their conditions in Article 43. Firms choose data categories (i.e. human resources transactional, or client data), their purposes, map data flows, describe storage periods, measures for data security and so on. Before, the process took anywhere from 1-2 years to complete and the costs reached the millions depending on the number of DPAs involved and the size of the company, which made them unpopular. The Regulation creates a more streamlined process under the consistency mechanism where national authorities and a new European Data Protection Board will coordinate approvals.

[e] The Article 29 Working Party (WP29) is a body of experts, DPAs, the EDPS, and European Commission that promote 95/46/EC's uniform application. The European Data Protection Board will assume its duties under the GDPR.

Standard Contractual Clauses have been used to transfer data to controllers and processors (intra-company and external) outside the EU.[f] Under 95/46/EC the Commission provided four types of SCCs – two from controller to controller transfers and one for controller to processor transfers. The Regulation retains the Commission's power to lay down SCCs, but also allows supervisory authorities to develop them in accordance with the consistency mechanism and with Commission approval.[26] The clauses must provide safeguards with enforceable data subject rights and legal remedies. The Directive required all affected DPAs to approve SCCs, but the Regulation does away with this obligation.

European interviewees stated that US companies preferred to forego SCCs, which forced European firms "try to include something that protects us regardless" noting that American corporations "don't trust them." US companies had the choice to use SCCs or become Safe Harbor certified, which favors the self-regulatory US privacy rules, and may explain the hesitation. In light of Safe Harbor's invalidation, SCCs became the favored option, while the industry awaits further details on the US and EU Privacy Shield arrangement (See Section 2.4).

2.3 Financial Privacy in the US

In the US, data is typically the property of the holder so ownership depends on the entity that possesses it. The Constitution does not explicitly mention privacy, but the Supreme Court has ruled that the Bill of Rights created "zones of privacy" within several Amendments including the 1st (freedom of speech), 3rd (privacy of the home), 4th (privacy of the person and possessions unreasonable searches and seizures), 5th (self-incrimination) and 9th (protecting rights not covered in other Amendments). As a result, the US regime has been developed by case law, in the form of torts, usually arising from civil complaints seeking damages to protect against invasions from the state on their person and property to preserve liberty - freedoms of expression, the prohibition of quartering soldiers, and the right to bear arms, and so forth.[27]

Most legal scholars recognize Warren and Brandeis's 1890 *Harvard Law Review* article "The Right to Privacy" as the origin for America's property-based privacy identity.[28] Written in response to a media account of a dinner given at Warren's home, the authors defined privacy as the "right to be let alone." They referred to European ideas of honor and reputation, but did not cite precedent for the violation of one's person through insult in US case law. Regardless, some academics have argued that the article suggests a US right to personality in the European tradition.[29]

[f] The European Economic Area, or EEA is party to many of these laws. It includes the 28 member States of the EU and Iceland, Liechtenstein and Norway who are part of the European Free Trade Association (EFTA).

Although Europe was the first to implement privacy law, the US was the first to create a template of Fair Information Principles (FIPs) in 1973.[30] The tort-heavy development of privacy rights produced a sectoral approach to data governance based on FIPs, which has been designed to inform individuals about the use of sensitive data.[31] For example, student education records in the 1974 Family Education Rights and Privacy Act (FERPA), medical records under the 1996 Health Insurance Portability and Accountability Act (HIPAA), or consumer communications records such as the 1966 Telecommunications Act, and the 1984 Cable Television Privacy Act. The sectoral model favours self-regulation and corporate control. Advocates say it is cost-effective and guards against regulatory burden for sectors outside these areas.[32]

Perhaps unsurprisingly due to the sensitive nature of wealth and money in US society, financial data has been among the most regulated types of information. Legislation targets maintaining accurate records and client access, corporate transparency, use control (with restrictions), and technological requirements to guard against breaches. Enforcement falls to a host of government entities. [33] The property-sectoral model gives the financial services a lot of control over their terms of service, and subsequently the ability to dictate the uses of customer data. Individuals have limited power over their data once they sign-up for services, a contrast to EU model that bestows data ownership to the individual. Generally, the US operates on an "opt-out" rule – individuals and their data are "in" unless they inform the company otherwise. US businesses must inform individuals of their rights (including that data is collected for AML/CTF purposes and may be reported) and any changes to company policies.

Thus, US privacy law is business friendly, flexible, and gives the financial sector data ownership rights, but it also promotes overlap and legislative gaps. This adds to the risks and costs of doing business since firms answer to multiple regulatory bodies that change according to product lines and geographic location. It can also lead to inconsistent applications of the law and muddled enforcement. A recent study of over 6,000 financial institution privacy notices showed huge variances in privacy policies, many companies offering conflicting information, and some failing to uphold the legal rights of consumers. Carnor et. al. recognized how the law could confuse "opt out" provisions noting, "GLBA's Financial Privacy Rule applies to the sharing of consumer financial information with non-affiliates, the FCRA restricts sharing consumer report information between affiliated companies, and FACTA limits when consumer report information shared between affiliates may be used for marketing."[34]

Like the EU, there is legal diversity at the US State level. Ten State constitutions – Alaska, Arizona, California, Florida Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington – explicitly mention privacy rights in some form.[35] Twenty-six States have data destruction

requirements, and many legislatures have enacted or are currently considering data breach notification laws.[36]

All US financial privacy laws contain disclosure and access restrictions for data collected, accessed, and used in criminal or national security investigations.[37] Unlike the EU, US AML/CTF law (e.g. the Bank Secrecy Act and US PATRIOT) does not explicitly require financial institutions to implement privacy protections in their compliance operations, with the exception of guarding against data breaches (including rules against disclosure).

In 2012, just after the EU announced its plans for the GDPR, the White House released a framework for consumer data privacy aimed at increasing "global interoperability" to provide individuals with more control over their data, more transparency in data usage with a respect for the context in which it is used, better information security, rights for access and accuracy, and an emphasis on focused collection and accountability. The Framework was predicated on the FTC's Fair Information Practice Principles (FIPPs) which granted it, and the State's Attorney's Generals, enforcement duties. The Obama Administration produced a discussion draft Bill in 2015 entitled the Consumer Privacy Bill of Rights Act, which maintains the US's property-based and corporate data ownership, exempts existing financial privacy laws and maintains police and national security access. Although the Bill makes strides to create some standards for how private enterprises manage consumer data, and lends individuals more control in certain circumstances, it has little bearing on how the financial services deal with AML/CTF data in the US.[38]

Table 2: US Financial Data Privacy Legislation

1970	Fair Credit Reporting Act (FCRA)	Accurate and relevant data in credit reports, sets notice requirements, allows individuals to access and correct data, requires agencies to investigate disputed information, and limits use. Must be able to opt-out of communication between affiliates about creditworthiness.[39]
1978	Right to Financial Privacy (RFPA)	Confidentiality of personal financial records under 4th Amendment. Requires appropriate written requests for information by authorities through subpoena, warrant, etc. Emergence of National Security Letters. Does not apply to state or local authorities, but some states have enacted laws to protect individuals from state investigations.[40]
1999	Financial Services Modernization Act (Gramm-Leach-Bliley, GLBA)	Title V. Businesses "significantly engaged" in financial activities must provide privacy notices, opt-out, and cannot sell pin or account numbers. Standards for security and record confidentiality. Governs "nonpublic personal information" (NPI) – data not generally publicly available that is provided to the FI by the consumer, results from a transaction in the business relationship, and when an FI obtains the data in connection with providing a service. FIs cannot forward this data to unaffiliated third parties, but there are exceptions. US States can adopt stricter measures.

	2003 Safeguards Rule	Requires security controls for financial institutions to protect paper and electronic records with "administrative, technical and physical safeguards"
2002	Sarbanes Oxley (SOX)	Concerned with financial accountability and standards and accuracy of financial statements.
2003	Fair and Accurate Credit Transactions Act (FACTA)	Amended FCRA to further restrict affiliate data-sharing. Designed to protect customers from identity theft; access to 1 free credit report annually; separated medical data from financial information and requires patient's consent for insurance enquiries. Prohibits sharing customer information for marketing and opt-out opportunity.
	2005 Disposal Rule	Requires appropriate measures to dispose of sensitive information derived from consumer reports.
	2007 Red Flags Rule	Development, implementation of identity theft prevention programs for creditors; FTC Sentinel database of consumer complaints[41]
	2008 Affiliate Marketing Rule	Affiliates may not use consumer report information received from an affiliated company for marketing unless consumer has been notified and given the opportunity to opt-out.[42]
2010	Consumer Financial Protection Act (Dodd-Frank)	Created CFPB to oversee credit agency reporting under FCRA, GLBA, RFPA and FPA. Regulates accuracy, reporting, and data security.

2.4: Safe Harbor and the Privacy Shield

For 15 years, the Safe Harbor arrangement governed transatlantic commercial data flows. Because the US did not fit 95/46/EC's adequacy standards, a Commission Executive Decision (2000/520/EC) created the Safe Harbor program that bridged EU human rights-based and US property-based privacy views. Safe Harbor did *not* apply to financial institutions as they are not regulated under the Department of Commerce (DoC), the Federal Trade Commission (FTC), or the Department of Transportation (DoT). Though it did not directly regulate financial data, Safe Harbor, and its successor – the Privacy Shield – do affect MFIs' risk relationships with third party vendors that provide and process data for them, which necessitates the arrangement's inclusion in this study. The European Commission did attempt to negotiate a financial Safe Harbor in 2004, but the effort failed due to a lack of political willpower within the Commission leadership and disagreements over the nature of US regulations.[43] US negotiators argued that the Gramm-Leach-Bliley Act, which required companies to issue privacy notices to customers and the option to opt-out of certain data sharing, already provided adequate protections for financial data.[44] Commission officials rejected this argument since individuals cannot control information-sharing with affiliates, third party service providers, or marketers.[45] Since then, financial institutions have relied upon on SCCs, BCRs, or operated under 95/46/EC's exceptions, but vendors do utilize the Safe Harbor scheme to legalize the collection, transfer, and processing of EU data (See Section 3.7a).

The program enabled companies regulated under the FTC or DoT to voluntarily submit to yearly certification after implementing seven principles including; notices to data subjects of the specified use and purpose of their data; the choice to opt out to data disclosure to third parties or to any use of their data that is "incompatible with the announced purpose"; safeguards for the transfer of data to third parties; individual access to data to correct, delete and amend it for inaccuracies; protection from "loss, misuse and unauthorized access, disclosure, alteration and destruction"; guidelines for relevant use; and finally a dispute resolution system for clients.[46] In 2013, after years of criticisms, the EU was pressured to revisit Safe Harbor's terms due to public pressure from Edward Snowden's disclosures of the National Security Agency's (NSA) PRISM surveillance program.[47] The EU offered 13 conditions for reform under four areas – Transparency, Redress, Enforcement, and Access by US authorities. All of these had been settled by the summer of 2014, but officials demanded that EU citizens enjoy redress rights under the US Privacy Act, due to concerns about transfers between private companies to the American government,[48] which may be resolved with the Judicial Redress Act making its way through Congress.[49]

More threatening to Safe Harbor's survival was the outcome of the Schrems v. Ireland case, where an Austrian law student filed suit against Facebook (which has offices in Ireland) alleging that Safe Harbor did not protect EU users from government surveillance in the US. The Irish DPA said it had "no duty to investigate" and the complaint was referred to the Irish High Court, which asked the Court of Justice of the European Union (CJEU) to clarify. In October 2015, the CJEU rejected the Decision on the grounds that American privacy law does not offer European citizens protection against US government intrusions.[50] The Court's decision was controversial as critics believed that the CJEU decision ignored recent US reforms that have curtailed US surveillance. And, as Member State national intelligence agencies are not covered under EU privacy law, some have argued that the ruling has exposed a double standard – forbidding transfers to the US for protections that EU citizens do not have in their own countries.[51]

Facing the possibility of fines and litigation, the US and EU reached a zero-hour agreement in February 2016. The new Privacy Shield maintains the DoC's oversight and monitoring duties for US companies, with enforceable accountability to protect EU data under US law. The most significant changes appear in the form of transatlantic cooperation between the FTC and DPAs, the creation of a "dedicated new Ombudsman" to address EU data subject complaints, and US government promises to "clear safeguards and transparency obligations" for data requests. US agencies' access to data will be regularly monitored and reviewed jointly by the DoC, the EU, national intelligence experts, and DPAs. There are, however, exceptions for mass surveillance that accommodate both US and EU

national security interests: where targeted surveillance is not "technically or operationally possible; or if a "dangerous new trend" emerged that demands it.[52]

3. COMPARATIVE ANALYSIS OF US & EU AML/CTF & PRIVACY LAWS

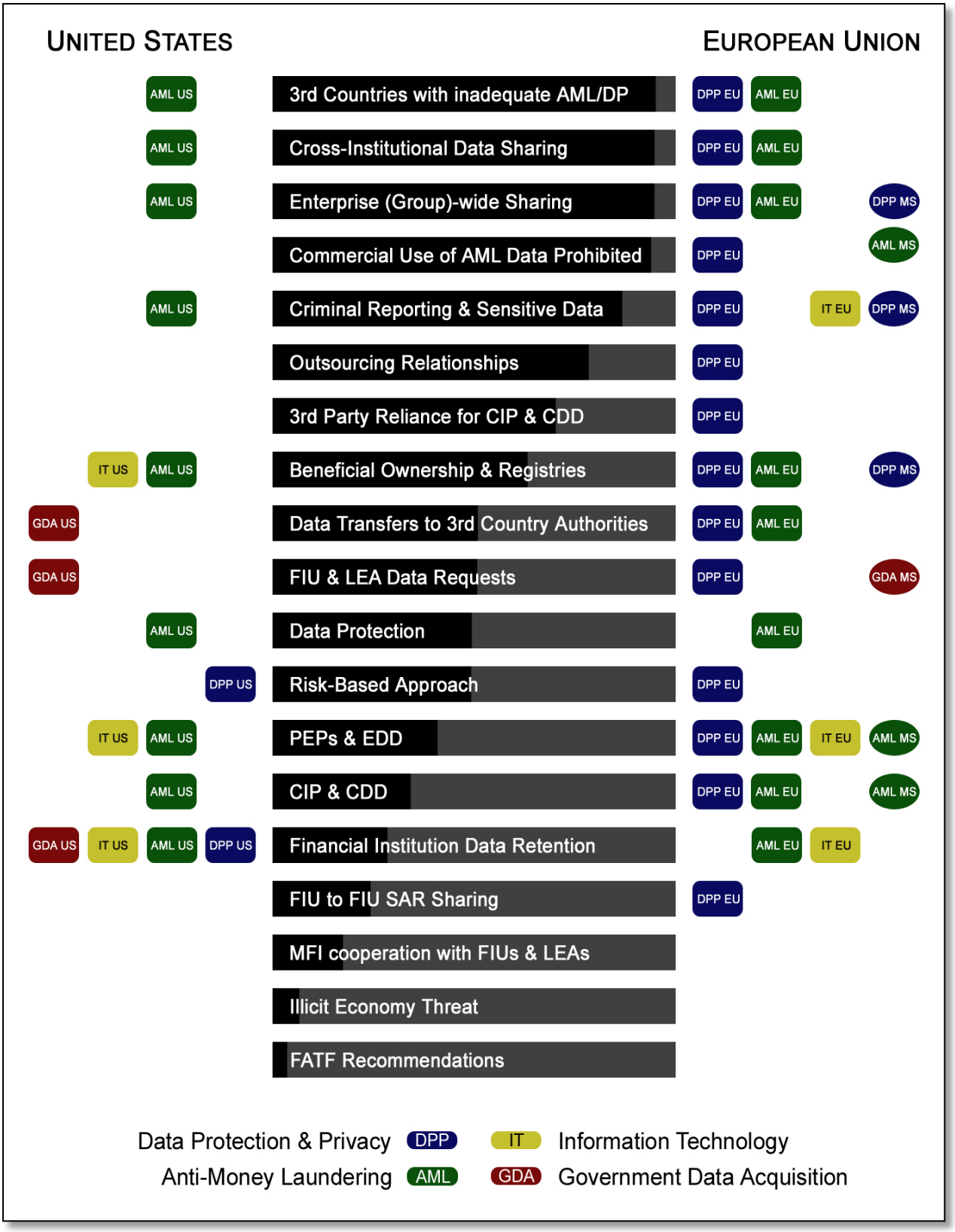
While the US and EU differ on privacy, transatlantic approaches to AML/CTF share greater symmetry because they were developed as part of a Group of Seven (G7)[g] initiative to combat money laundering in the drug trade. Since its inception in 1989, the Financial Action Task Force (FATF) has set 40 Recommendations that constitute the backbone of national and industry efforts to combat the illicit economy and terrorist financing.[53] FATF rule-making involves consultations with government members and industry experts. Like any attempt to create globally implementable standards, inter-state differences and divergences among market practices have necessitated broad, rather than narrow, norms. As a result, FATF Recommendations have produced variances among national legislation, so it is of little surprise that industry practices shift constantly to keep in tune with local demands.

In the US, the Bank Secrecy Act and Title III of the US PATRIOT Act constitute the main pieces of AML/CTF legislation. They are primarily overseen and directed by the US Financial Intelligence Unit, the Financial Crimes Enforcement Network (FinCEN), within the Department of the Treasury. Like the US privacy regime, the US AML/CTF regime is dispersed in rule-making and enforcement. FIs are governed by regulatory authorities (with accompanying statues and rules) that shift depending on the FIs functions (i.e. The Federal Reserve (FED), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Securities & Exchange Commission (SEC), and National Credit Union Administration (NCUA).

The Europeans have a slight advantage because 4AMLD sets some regional legal and definitional baselines for compliance across the region. However, a Directive requires the Member States to transpose these requirements which invites national interpretations, which force multinational firms to tailor compliance to local expectations. Furthermore, as the GDPR allows Member States to set limitations and determine appropriate safeguards for data protection in compliance, firms will also have to implement privacy at the national level in some capacity.

[g] G7: United States, United Kingdom, France, Germany, Italy, Canada, and Japan. See Frasher, 2013 for the policy-making dynamics within the Group in monetary affairs.

Table 3: Transatlantic AML/CTF & Privacy Conflicts

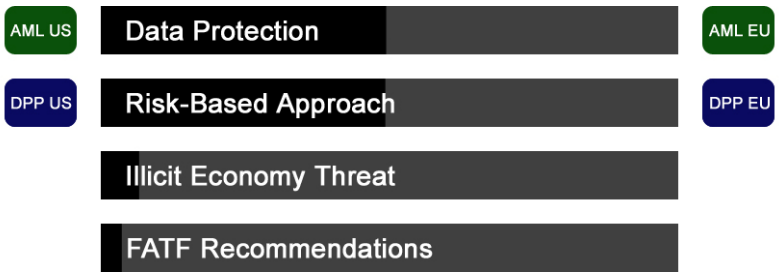


Although US and EU firms contend with AML/CTF regulatory multiplicities, the FATF produced shared operational and definitional foundations whose differences are trivial compared to those found among transatlantic privacy regimes.

This section presents an analysis of 19 compliance areas from an appraisal of US *federal* and *EU-level* AML/CTF and data privacy legislation, which illuminated strengths, weaknesses, and risks within, and between, both regimes. Chart 3 summarizes the results, with bars filled to various degrees of black to indicate the severity of MFI risk due to conflicts between data privacy and AML/CTF legislation, or where there are noticeable gaps in either US or EU AML or privacy requirements. Because US AML law does not require data privacy, this alone created legal discord and operational risk at every point in the study. For these reasons, and because exposures shift according to each institution's role and function, the analysis broadly evaluates the degree to which privacy may impact and institution's AML/CTF and privacy efforts. Icons on the left and right flag legal issues with US law and EU legislation.

As neither EU privacy law nor 4AMLD help the financial industry identify privacy obligations within their AML/CTF operations, this omission compounds multinational regulatory risk, but also creates an opportunity for FIs to instigate best practices. The exercise is meant to help those efforts move forward and demonstrate areas that represent legal barriers that create operational difficulties between US and EU compliance to advance an understanding of the challenges involved in implementing privacy programs within AML/CTF operations.

3.1: 2012 FATF Recommendations; Illicit Economy Threat; Risk-Based Approach (RBA); Data Protection



The US and EU have committed themselves to the FATF Recommendations recognizing that the illicit economy and transnational political violence are a threat to their economic well-being and national security. Within the BSA,[54] Title III of the US PATRIOT Act, and 4AMLD, the transatlantic partnership has adopted a Risk-Based Approach (RBA) rather than a rules-based

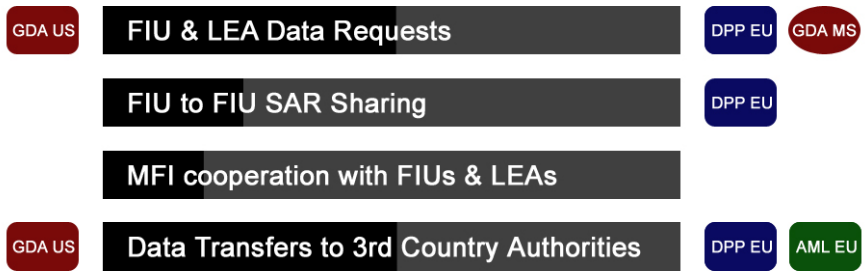
approach for compliance that helps multinational financial institutions (MFIs) create more consistent enterprise-wide programs. The FATF explains the RBA,

> When assessing ML/TF risk, countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CFT measures. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CFT risks, but it is still used for ML or TF purposes.[55]

In the RBA, governments believe that finance "knows its business best" and the method gives MFIs control over reporting, but it also serves as the origins for many of the legal and operational conflicts described below. RBA allows regulatory authorities to engage in their own assessments of how well FIs determine these risks, which opens corporate practices to various levels of scrutiny.[56] The legal and operational uncertainties of the RBA such as, "am I under reporting or over reporting?" can expose firms and compliance officers to fines, litigation, and reputational damage when regulators do not agree with the appropriateness of their methods. In some cases, this results in a "technology or methodology race" where regulators pit the methodologies of one institution against each other in the course of their assessments (intentionally or not). One senior compliance officer explained, "Sometimes regulators will compare our processes with others and ask 'Well, X is doing this and using this technology, why aren't you doing the same?'"[57] Several members of consultancy firms support these anecdotes, noting that their clients frequently ask "What is everyone else doing?" during their consultations. It seems that even as the industry does not often openly collaborate on their methods, it inadvertently creates standard responses, albeit in an informal and piecemeal way.[58]

There are few legal differences between US and EU RBA strategies, which denotes RBA's low risk position in the chart. But the legal conflicts rise substantially when one places the EU's rules-based data protection regime within AML/CTF risk-based operations. Furthermore, EU privacy law is meant to be applied with *limited* exceptions, which cause problems with RBA methods that involve collecting and analyzing volumes of personal data to determine risk. This dichotomy, and the fact that the US does not require data protection controls (beyond information security) to be implemented in AML/CTF compliance guarantees legal and operational conflicts in nearly every issue area.

3.2: MFI Cooperation with Financial Intelligence Units (FIUs) & Law Enforcement Authorities (LEAs); FIU to FIU SAR Sharing; FIU & LEA Data Requests; Data Transfers to Third Country Authorities



Close ties between public and private bodies ensure successful AML programs and valuable information to authorities that enable better interstate FIU cooperation. Good relationships, and strong legal incentives to comply (usually fine-based), have been essential tools for states to employ Information Statecraft to gather data from the private sector.

Section 314(a)[59] of the PATRIOT Act enables authorities to acquire "lead information" which is "not a substitute for a subpoena or other legal process.[60] The Section allows US federal, state, local, and foreign LEAs (since 2010) to submit information requests to FinCEN, which determines if the information is related to ML/TF, and then notifies FIs (about every two weeks) to check a secure Internet web site. Participation is mandatory and FIs are required to conduct a one-time search for client accounts in the past 12 months and transactions within 6 months, and respond within 2 weeks only if they find positive matches. If LEAs want to access the information associated with a match they must apply appropriate legal means. Requests are confidential and cannot be shared with a foreign branch office or affiliates. According to sources familiar with § 314(a)'s making, it was supposed to encourage "two-way" data-sharing among LEAs and the private sector, but has "fallen short of expectations." ("We expected more feedback about investigations so we could improve reporting.")

Subjects are only "reasonably suspected" based on "credible evidence" of engaging in terrorist acts or money laundering" and FinCEN advises FIs not to file SARs based on these enquires. Interviewees monitor these accounts a little more closely and then decide whether to file a SAR based on risk. However, unlike Office of Foreign Assets Control (OFAC) alerts and its Specially Designated Nationals (SDN) list that notify FIs of natural or legal entities restricted under US and other sanctions, § 314(a) lists are "…not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated." The one-time search and the requirement for documentation puts § 314(a) at least partially in line with EU privacy concerns, which favors case-

by-case, rather than bulk, requests. Yet, the presence of a *suspected* subject's name on outdated government to FI lists, "some names were on § 314(a) for years, and the distribution email lists weren't always kept current," and the broad nature of what could be considered lead information would raise eyebrows in the EU since § 314(a) challenges European data collection, retention, deletion, purpose limitation, or access requirements.

In Europe, 4AMLD Recital 57 and Article 42 obligate MFIs to "respond fully and speedily to enquiries from their FIU or from other authorities, in accordance with their national law." Some Member States only allow FIUs to make additional data requests from FIs that have already filed reports, when responding to a foreign FIU request, or through court authorization. The discrepancies among national laws complicate data collection for authorities, and complicate compliance for MFIs who must be aware of what can and cannot be shared with authorities depending on the jurisdiction in which they report and operate. In the wake of the November 2015 Paris attacks, France has called attention to this problem. A French Embassy document cites 4AMLD Articles 32 and 33 and FATF Recommendation 29 as legal grounds to harmonize FIU data collection and right of disclosure to include FIs that have not directly filed STRs,[h] but may have valuable information in order to strengthen the ability of European FIUs to track terrorist finances across the region.[61]

95/46/EC and the GDPR do not have jurisdiction over LEA and FIU data collection within the Member States. The Regulation says that public authority requests "should always be written, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems,"[62] but it does not cover that data once it is in LEA hands. The management of LEA and FIU data is guided by Council of Europe Recommendation R (87)15, (influenced by the standards set forth in Council of Europe Convention 108), which asks Member States to treat police data to the same conditions as personal data. The "(Role of Law) Police Uses of Personal Information Across Europe," or PUPIE project, sponsored by the Council of Europe found that while R(87)15 had been widely applied within Member State law and practice, there was a need for better enforcement and harmonization across the region.[63] Inter-EU LEA and FIU exchanges are governed by Council Framework Decision 2008/977/JHA, but it does not apply to data collection *inside* the Member States. In tandem with the GDPR, the EU has agreed upon a Police Data Directive (PDD) will help cover data protection gaps within Member State laws and better synchronize criminal and LEA data processing. Hence, the PDD may help firms develop more consistent policies when complying with EU LEA requests.[64]

[h] FIUs require FIs to submit many types of reports pertaining to financial transactions that were completed or attempted where compliance professionals feel that there is a risk of ML or TF. Their names, when to file, and data required, change according to the jurisdiction. Examples include; Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), Unusual Transaction Reports (UTRs), and Currency Transaction Reports (CTRs).

4AMLD prohibits FIUs and LEAs from directly requesting data from FIs external to their jurisdictions and to use official channels when they need information held by a FI in another state. As 4AMLD requires EU-based institutions operating in the US (and the globe) to implement enterprise-wide SAR and data-sharing programs with EU AML/CTF standards in place, EU data stored or accessible in the US is subject to acquisition by US authorities via subpoenas under the Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act (FISA) requests, National Security Letters (NSLs), Executive Order 12333, and PATRIOT §§ 702, 703, 704, among others.[65] MFIs are prohibited from acknowledging the existence of these requests as well as SAR investigations or filings (and protected from civil suits).[66] Individuals outside immediate compliance circles and the data subjects themselves would not be alerted to these actions, and privacy advocates are concerned about US "onward transfer" data sharing to allies or other entities as well.[67]

Europeans also complain that US authorities extend their data collection reach on foreign accounts through PATRIOT § 319(b). Section 319(b) enables the Attorney General or Secretary of Treasury to "issue a summons or subpoena to any foreign bank that maintains a correspondent account in the US for records relating to such accounts, including records outside the US relating to the deposit of funds into the foreign bank." FIs have 120 hours to deliver the requested information.[68]

Again, authorities in the US and EU are careful to specify that LEAs and FIUs should not approach FIs in other jurisdictions directly and to only communicate on investigations or share SAR data via appropriate official networks like the Egmont Secure Web or, within Europe, the EU FIU.net.[69] Egmont Group guidelines state that FIUs should establish Memorandums of Understanding (MOUs) that outline the nature of FIU to FIU cooperative relationships that include data-sharing.[70] Since 2010, the US and EU have negotiated an "Umbrella Agreement" (UA) to cover data transfers from EU authorities to US authorities, but critics note that the present text contains broad allowances for transfers and further processing beyond LEAs to national security groups and no "human rights" clause to protect individuals from errors or misuse. Private companies should note that the Umbrella Agreement will not protect European US branches from EU scrutiny over these kinds of requests, but US law requires that they comply accordingly.[71]

The UA (yet to be adopted) was contingent on the US Congress passing the Judicial Right to Redress Act (HR1428).[72] The Act, which was finally passed and signed by President Obama in February 2016, provided EU citizens redress rights for data held by US authorities. Before this, American citizens enjoyed these rights in the EU, but EU citizens could not exercise these rights under US law.[73] The measure gives a "covered" country's citizens the right to civil action against the US federal government in accordance with the Privacy Act of 1974, but only in "respect to

disclosures intentionally or willfully made" that are "contained in a system of records" (with exceptions) when the federal agency refuses access or rejects an individual's right to request amendment.[74] The Act designates "covered" countries, or "regional economic integration organizations" as entities that have "entered into an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses." The Senate amended the text to stipulate that a covered country must "permit commercial data transfers with the United States and may not impede the national security interests of the United States." The Attorney General with the concurrence of the Secretaries of State, Treasury and Homeland Security, may remove the designation if the country "impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person."[75] but what constitutes an impediment is not defined. The Act prohibits the disclosure of "classified information" and allows for a one-sided court review, "in camera and ex parte any submission by the agency in connection with this subsection," which suggests that data relating to AML is not applicable since it cannot be disclosed. If an investigation or the presence of a SAR is unintentionally disclosed, the court and agency are the only parties that can review the document in court. This is comparable to EU law since 4AMLD does not allow individuals to access SARs.

A caveat on Member State national security and intelligence agencies – they are *not* subject to the GDPR, 2008/977/JHA, R (87)15 or the new Police Data Directive.[76] This omission contributed to the Safe Harbor invalidation controversy, and critics of the CJEU decision have pointed out that the Member States themselves do not provide the kinds of protections demanded of the US. Because the AML/CTF regime demands a close working relationship with the criminal justice and national security communities on both continents, the legal ambiguities involving national intelligence gathering and third country transfers make it difficult for MFIs to avoid risk.

3.3: Customer Identification Program (CIP) & Customer Due Diligence (CDD)

Know-Your-Customer (KYC) begins with a Customer Identification Program (CIP) that gathers enough data to identify a client[77] or potential client.

CIP data is placed in context of other information to help FIs determine the customer's risk profile, which is monitored throughout the course of the relationship.

FinCEN's 2014 proposed rule focuses on four core CDD elements; 1) identification and verification of customers, and (2) beneficial owners and legal entities, 3) the nature and purpose of those relationships, and finally 4) ongoing monitoring.[78] US 31 CFR § 1020.220 outlines CIP data for depository institutions that must be collected during the onboarding process – name, date of birth, residential or business address, taxpayer, passport or government ID number.[79] Existing customers are exempt if the FI has a "reasonable belief" that it knows their true identities, but it depends on the bank's risk assessment of the account. In US privacy law, individuals can access, verify, and correct some account data under FCRA, but FCRA, the BSA and its accompanying regulations impose access limitations on FIs for AML processing. Unlike the GDPR's provisions on profiling safeguards (See Section 4), FCRA access would not cover a FIs BSA required monitoring practices in the US.

For ID verification, 31 CFR § 1020.220 instructs banks to use documentary and non-documentary methods for verification, due to the "availability of counterfeit and fraudulently obtained documents." FIs can collect multiple documents and compare them with data "obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement."[80] Many banks use vendor databases for this function, which pose their own data protection risks (See Section 3.7a).

4AMLD requires identifying information but the Directive offers limited guidance on what types of information should be mandated in national law.[81] While some Member States specify what data should be collected, others simply ask FIs to be able to adequately identify the customer, and many times criteria are left to the FI's discretion "on a risk sensitive basis."[82] Identity verification under both regimes is subjective and neither US law nor 4AMLD provide FIs with standards to confirm an individual's identity. The EU asks Member States to warrant "reasonable measures" but admits these may change according to the "risk profile" of the customer (e.g. location of client, market, type of product) so additional data collection may be necessary.[83] Verification is also left to FI discretion as it does not need to "establish the accuracy of every element of identifying information obtained" as long as it has a "reasonable belief" (not defined) to know the "true" identity of the customer.

The AML Directive limits individual access to the processing of data to protect FI compliance obligations and to ensure SAR confidentiality. Article 41 allows Member States to restrict "…in *whole or in part*, [emphasis added] the data subject's right of access to personal data relating to him or her to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person…" Instead, Recital 46 and Article 41 allows supervisory authorities to act as a go-between and contact FIs, LEAs, or other supervisory authorities to access an individual's data in the course of

AML/CTF processing to determine the "legality" of the processing.[84] Under 95/46/EC and the GDPR, customers have the right to access to check the accuracy of their account data, contest it, and make corrections to data utilized for commercial relationships. It is unclear where legislators and regulators would draw the access line between CIP and CDD.[85]

Because firms want to make sure that they can prove adequate due diligence, the quality (and sometimes quantity) of data an FI possesses on an individual or entity is vital part of what constitutes a strong CDD and EDD program. US FIs are required to notify customers of their AML/CTF data collection obligations, which is also the case in Europe. However, firms can decide to ask for information beyond these requirements such as the purpose of the account, the source of funds, additional sources of income, occupation, and the details of other banking relationships.

3.4: Politically Exposed Persons (PEP) & Enhanced Due Diligence (EDD)

In an effort to detect and halt money-laundering, tax evasion, bribery, or terrorist financing for those in political leadership positions, the FATF request national governments conduct EDD on clients acting in both domestic and foreign public roles.

The definition of a PEP changes according to the jurisdiction. The US considers a "senior foreign political figure" in any branch of government, elected or not elected, their immediate families and close associates a PEP. US law places greater compliance measures on foreign officials when they want to open accounts in US banking institutions. There is no official definition of a domestic PEP. FinCEN has chosen to place domestic political officials in the context of a FIs CDD practices and leave it up to the bank whether to impose additional measures based on a client risk assessment. FinCEN notes that the definition "must remain sufficiently flexible" so that banks can monitor those who may be in the position to gain from the proceeds of corruption.[86]

4AMLD defines PEPs, but Member States can expand these criteria and compose national lists of leaders (e.g. some states and FIs list football players as PEPs). Monitoring is not limited to PEP themselves, which places FIs in the position of delving quite deeply, and sometimes embarrassingly as interviewees recounted, into the personal lives of their political clients. Family members, including children and their spouses, are included and the FATF suggests that "close associates" or persons "(known) (sexual) partners outside the family unit (e.g. girlfriends, boyfriends, mistresses) …" should be included in the risk profile. 4AMLD does not define close associates in this detail, instead choosing to use the language "equivalent of a spouse." In the US, the FFIEC BSA

Manual refers to close associates as "a person who is widely and publicly known to maintain an unusually close relationship" with a PEP.[87] Probing the personal relationships of PEPs and their families to the extent that MFIs are chronicling their sexual lives dips into the sensitive data categories protected by the GDPR in Article 9 because such information denotes one's sexual orientation or sex life and requires explicit consent (Section 3.8). The EDPS and WP29 expressed concern about PEP requirements believing it an invasion of privacy beyond what is necessary for AML compliance.[88] Their worries regarding the proportionality of data collected, profiling, discrimination and data retention are salient as there are no limitations to the length of time one can be designated or monitored as a PEP. Since PEPs require constant monitoring and their profiles will contain sensitive data, this further qualifies the need for a data protection officer under the GDPR's terms.

FIs must be aware of, and frequently check, government issued lists when available, as well as keep tabs on any changes in a PEP's status. A 2015 ACAMS/Dow Jones survey indicated that this has become a common practice with 75% screening for domestic PEPs and 90% looking for local level leaders. Measuring PEP risk should involve a two prong approach that accommodates FATF foreign and domestic PEP requirements. MFIs should assess PEPs via *national* risk profiles that examine the prevalence of corruption within their state, the level of organize crime and governmental transparency, and the type of political system (e.g. autocratic systems typically operate on patronage relationships). Then, they should place PEPs in an international context to determine whether the country is or the FATF's blacklist, which designates states with less stringent AML legislation and enforcement, or under UN sanctions.[89]

There is debate about how long to keep PEPs are PEPs to cover IFI risks since it is difficult to keep track of when PEPs enter and leave office to maintain bank records- "Once a PEP always a PEP."[90] Furthermore, 4AMLD requires banks to maintain EDD for *at least* 12 months after public service, but Member States can extend this time.[91] Family members are not included in the 12-month observation period, which leaves the possibility that former officials can just reroute funds to relative after the expiration. The US, however, leaves PEP duration up to the bank's risk assessment.

3.5: Beneficial Ownership & Registries

CIP, CDD, and EDD are essential to determine Beneficial Ownership (BO). BO refers to a person or group of persons who benefit from financial accounts that include natural persons, legal entities, trusts, and unincorporated associations.

BO rules are aimed at promoting transparency to certify that these persons and groups are not engaged in hiding dirty money or acting as vehicles to move funds for terrorist organizations.[92]

Both 4AMLD and FinCEN's proposed rule set a 25% minimum interest on a natural person or corporate entity when determining ownership in a company. Europe does allow Member States to set the bar lower.[93] When no single individual meets those criteria, the bank must maintain CDD of the company's senior management, which may be determined, inter alia, by 2013/34/EU[94] where for example "a shareholder agreement between a 20% and 10% shareholder leads to control senior management as Ultimate BO is a last resort."[95] FinCEN has proposed a two prong method to determine BO. The first prong determines *ownership* for each entity with 25% minimum interest (maximum of 4). The second prong determines *control*, such as a manger or executive officer, where one person must be listed. An entity with 25% ownership and 25% control can be recorded under both prongs. Some have criticized thresholds believing that criminals can simply structure a company so no one meets the minimum.[96] In these cases, it is left to the FIs risk assessment whether to list those with less than 25% interest which places more responsibility upon the compliance program, and leaves FIs open to subjective regulatory measures.

Identity validation in BO is also an issue for FIs. 4AMLD mandates "reasonable measures" with "reliable and independent source[s]" to verify documents before taking on the relationship and to constantly maintain these records.[97] For US banks, the risk of establishing a BO relationship upon fraudulent information is greater than the EU since the proposed FinCEN rule would allow the use of a standardized form, which requires the individual opening the account to certify that the information provided is "true and accurate to the best of their knowledge." The proposed FinCEN rule only requires that FIs verify identities, not the status of the BO.[98] Banks are not obligated to follow-up unless they determine that the client is a risk, which again leaves them vulnerable to regulators. The rule noted that there were no limits on how supervisory authorities might judge a FIs CDD and BO requirements and interviewees remarked that regulators do inquire about verification methods during examinations.

While the US and EU agree that determining BO is important,[99] they have taken different approaches to the transparency of this data. 4AMLD requires Member States to host BO data in central national registries that can be directly accessed and updated by MFIs, or by supervisory authorities. MFIs will have to establish relationships in each jurisdiction that reflect the method chosen by each Member State. The US initially decided not to create a central storehouse for BO data, but is now reconsidering this in the wake of the Panama Papers scandal that exposed hundreds (thus far) of individuals who attempted to use shell companies to hide corporate and personal investments and profits.[100]

Member States may decide to create publicly accessible databases or limit access to persons with a "legitimate interest," is left to the discretion of national law. In its early reviews of 4AMLD's draft, the EDPS advocated for the right to access to correct inaccuracies. The EU took these concerns into account, especially pertaining to the protection of minors and beneficiaries of trusts, permitting exemptions "where such access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation, or where the beneficial owner is a minor or otherwise incapable."[101] The GDPR permits data transfers to registries with appropriate safeguards, but still does not define what constitutes a legitimate interest for access.[102]

Interviewees in US firms suggested that European-based companies may enjoy less liability for identity validation because there is the possibility to share responsibilities with Member States in managing the registries. Advocates say that state-managed registries heighten the danger of security breaches, while supporters claim central registries would help uncover shell companies, anonymously held, which are prohibited in the FATF Recommendations.

3.6: Financial Institution Data Retention

MFIs must create secure data systems with adequate storage to quickly locate[103] and deliver information to LEAs and FIUs, and to conduct enterprise-wide KYC, transaction monitoring, and if necessary, investigations. Data retention demands carry tremendous technological and staffing resource burdens to store client data, transaction data, SARs, investigation analysis, and communications with authorities.

US and EU data retention requirements for FIs are comparable. The EU requires data to be held for 5 years with a possible extension of another 5 years, but limits retention to a total of 10 years. 4AMLD also requires Member States to assure that FIs have "specific safeguards" in place to "ensure the security of data and should determine which persons, categories of person or authorities

should have exclusive access to the data retained."[104] It does not provide technical guidelines and administrative measures for data retention or breaches, but other pieces of legislation and industry-led standards fill these gaps.[105] The data retention demands are consistent with GDPR requirements that data is not kept longer than necessary and that there be internal procedures for data rectification, storage, and erasure with periodic review. AML/CTF data retention periods cannot be shortened by the GDPR's "right to be forgotten" (erasure) provisions because it is saved for "legal obligations" and "reasons of public interest."[106] However, the Regulation does oblige firms to notify supervisory authorities of a data breach "not later than 72 hours after having become aware of it" and to data subjects especially when their rights and freedoms may be compromised.[107]

On the US side, FI data retention is typically 5 years but can be extended to 6 years or longer if requested by the Secretary of Treasury. In addition to SARs, transaction data, KYC, CDD, EDD data, the US requires banks to retain SAR acknowledgements for 30 to 60 days, Alerts for 30 days, and Track Status Data for 5 years. US PATRIOT § 326 requires FIs to hold account data (copies of IDs and other documentation) for 5 years after the account is opened, and credit card data for 5 years after the account is closed or dormant.[108]

FIs must employ technological and administrative processes to maintain records to accommodate storage durations which will change on the location of their client and operations, which will increase costs. They should also consider the location of their servers and the data protection requirements associated with storing EU citizen data or claims by authorities in one jurisdiction to data held abroad by US-based firms.[109]

3.7: Third Party Reliance for CIP & CDD[i]

Colloquially, a third party refers to a variety of players. It can denote members of the financial services covered under AML regulation, federations of FIs, and vendors that support AML/CTF or privacy operations.

Legally, and for the purposes of this Section, 4AMLD defines third parties as obliged entities[110] and federations of obliged entities that apply CIP and are supervised under an EU regulatory authority. Article 25 of the Directive dictates that Member States permit FIs to rely on third party FIs for CIP, and notes that "the ultimate responsibility for meeting those requirements

[i] It is beyond the scope of this paper to address all types of third party outsourcing. Vendors play diverse roles and their relationship with data protection laws will be unique.

shall remain with the obliged entity which relies on the third party." Like privacy controllers and processors in the GDPR, the FI handling the relationship is ultimately held accountable for the security of that data. Under the Regulation, an FI must notify potential customers and current customers that their KYC data may be shared in this manner and make appropriate arrangements for these transfers depending on the locations of these relationships. These inter-firm transfers may fall under the GDPR's exceptions for the performance of a contract, necessary under law, or for national security investigations. It is unclear how Member States will interpret these transfers or apply the GDPR's safeguard requirements.

For compliance, 4AMLD's third party blessing can be helpful to create consistent and thorough KYC processes across groups and among the financial services. To avoid having the customer repeatedly provide customer identification, the US and EU authorize a FI to use data from other institutions *if they are part of the same group and subject to the same AML rules*. The EU includes affiliates and subsidiaries in third countries (with responsibility resting on the obliged entity to make sure that requirements have been fulfilled), but 4AMLD does instruct Member States to prohibit obliged entities "from relying on third parties established in high-risk third countries." There are exemptions only "where those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures." In contrast, there are no explicit exceptions in US law for high-risk or AML equivalent states, but since the US does not recognize foreign branches under BSA it suggests that all foreign branches are high-risk (even in the EU) since domestic entities cannot legally rely on KYC conducted overseas, which also causes problems for US branches overseas (See Section 3.10b).

US firms can use another domestic financial institution, including affiliates, to collect data and verify customers if they are subject to AML rules under 31 USC § 5318(h)[111] and are under a federal functional regulator; if the customer already has an account at either institution; if it has a contract with a third party; and finally, if the "reliance is reasonable under the circumstances." In the event that they use the "reliance provision," including having third parties manage records, the bank must make sure that the third party is not under enforcement actions that might undercut their reliability. Similarly, for commercial financial data, there are no restrictions for sending customer data abroad for third party processing. Under the Gramm-Leach-Bliley Act, FIs do not have to disclose these practices but they are legally responsible to ensure that joint service providers "maintain the confidentially" of that information abroad.[112] As the US law does not prohibit FIs from using KYC data for commercial purposes, and there are no privacy provisions in US AML law, EU client data may be forwarded to these service providers without European-level protections unless the firm has SCCs in place for that data.

3.7a: Outsourcing Relationships

4AMLD considers third party vendors "outsourcing relationships" or "outsourcing service providers" whose interactions with FIs are set by contractual agreement. Their legal status is separate from third party FIs described above.[113] Again, US and EU FIs are accountable for the actions of outsourced services, whether or not the services are directly regulated under AML law. AML support vendors are a multibillion dollar industry - auditing, payment processing, transaction monitoring, fraud detection, KYC registries, customer identity management systems, databases of client-oriented information used for CDD and EDD onboarding and maintenance, PEP status monitoring, matching individuals to sanctions lists, information security, and data storage to name a few. Developing data provider capabilities is cost-prohibitive for FIs so there is a heavy dependency on these services. This dependency carries AML and data protection risk.

4AMLD allows Member States to authorize vendor and outsourcing relationships with legal responsibility for data protection and AML compliance resting upon the contracting institution. Using service vendors to process data is consistent with 95/46/EC[114] and the GDPR, and these companies must implement technological and organizational safeguards. The provision that controllers must make sure that processors do not subcontract work and that they are also legally accountable adds another layer of vendor management to the AML/CTF data equation.[115]

Among the most prominent examples of third party AML services are vendors who offer databases of open-sourced customer information that banks use for non-documentary (in BSA parlance) CIP verification. A 2015 ACAMS/Dow Jones survey showed that 70% of respondents depended on outsourced data providers, and more than 55% used multiple vendors.[116]

Companies that collect open-source data for KYC databases used in CDD or PEP monitoring individually *identify* a client and the purposes for which they use the financial system. Commonly understood, open-source data refers to "data that is publicly available" including newspapers, books, broadcast or reports, which are written by many kinds of authors – academics, citizens, governments, journalists for example. Open-source data is not immune from data protection as the law is at its most potent as it applies to PII, and there are some notable cross-Atlantic privacy ambiguities.

Directive 95/46/EC and the GDPR take a broad approach in defining PII.[117] Open-source data is subject to data protection when it becomes personal data – when it can identify and individual or his/her behaviors – and then becomes protected under data protection law.[118] The GDPR text adopts

this view and applies to "any information concerning an identified or identifiable natural person" and specifically references "one or more factors specific to the physical, physiological, genetic, mental, *economic*, cultural or social identity or that person."[119] The designation of the economic indicator indicates an awareness of the impact that financial practice, and compliance, may have on an individual's fundamental rights.

Identification is not the only concern; using open-source research methods also raises the possibility of inaccuracies. Industry polls reveal that data accuracy consistently ranks among the highest concerns for AML/CTF data vendor outsourcing.[120] "It's not a question of the technology, it's the content, the data, that matters, and that's where clients [and banks] focus."[121] Under EU law, individuals have the right to access these services and correct inaccurate data, and these rights may be enforced by the GDPR (See Section 4) where persons are affected by legal decisions taken by automated and semi-automated processing. The Regulation also requires controllers to notify data subjects "where personal data have not been obtained from the data subject," the type of data and processes involved, and when there may be the possibility of onward data transfers to third countries and whether those countries have adequacy decisions.[122]

The US approaches PII in several ways; a) tautological (law that indicates data specifically "identifies a person"); b) non-public (privacy law that excludes any information that is publicly accessible); and c) specific types (laws that enumerate exact types of data to be protected).[123] These distinctions are important because where the EU protects data that identifies, or has the potential to identify a person directly or indirectly, the US does not. For example, if one defines PII in accordance with the GLBA's description of non-public information – "then publicly accessible data" is excluded from US protections. However, the GLBA does not apply to third party vendors as they are not considered financial institutions. Database providers are susceptible to FCRA regulation though. Even as they do not provide the same types of information as credit reporting authorities to individuals, they do furnish such information to insurance companies and banks which may decide to deny services based on this information.

Many of these services were certified under the invalidated Safe Harbor program and currently depend on SCCs until the new Privacy Shield goes into effect. Although an IAPP/EY survey of privacy professionals showed that 85% of respondents working in the banking industry had a vendor management program, MFIs should examine vendor policies and legal protections.[124]

3.8: Criminal Reporting & Sensitive Data

The GDPR Article 9 defines "special" categories of data as "personal data revealing racial origin, political opinions or religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person concerning health or sex life and sexual orientation shall be prohibited."[125] Article 9(a) cites criminal data as a special category and specifies that its processing must be "kept under control of an official authority" which does not address data that might be collected in the course of a FI's AML/CTF compliance or garnered through a vendor's CIP databases.[126]

ML and TF employ many methods to raise, collect, hide, and transfer funds, and national laws identify a multitude of predicate offenses that FIs must monitor for SARs and other reports. US law criminalizes a host of "unlawful activities" that include tax code violations, fraud, terrorism, identity theft, bribery, embezzlement, murder, kidnapping, robbery, extortion, destruction of property, sexual exploitation, child pornography, trafficking, smuggling, assassination, violence at international airports, drug trade, arms control violations, and even environmental crimes.[127]

4AMLD's list of applicable "criminal activities" limits data collection that refers to terrorist offenses, narcotic drug manufacture, transport, cultivation and sale, criminal organizations, corruption, misrepresentation of financial interests in documents, fraud, and tax crimes. In addition, MFIs are required to share these suspicions within the group to promote cohesion in reporting so some of this data may reach the US through affiliates and subsidiaries of EU firms.[128]

The exhaustive list of criminal offenses allows a wide net for US data collection within the AML regime, which not only adds to the costs of compliance, but causes MFIs to violate EU proportionality principles and edges compliance's function creep – acquiring data for use beyond its intended use for ML and TF prevention and detection.[129] The collection and possible transfer of criminal conviction data may violate Member State rules. Unfortunately, 95/46/EC did not address this issue and the GDPR covers "commercial sector organizations," their need to process criminal data to combat financial crime, and third party vendor data,[130] through vague language that allows processing "authorized by Union law or Member State law." The GDPR stipulates that criminal data must be protected by "adequate safeguards." However, the exact nature of these safeguards, as well as the exceptions for the "public interest" will vary across the Member States.

3.9: Prohibition of AML Data for Commercial Use

The EU's prohibition on using AML data for commercial purposes presents one of the highest risks to FIs because AML/CTF data is a treasure trove of information that banks could use to identify markets, new products, to tailor services to clientele, and many other uses not related to ML or TF. However, marketing and other uses is not the intended purpose for collecting KYC data and it is *expressly prohibited* under Recital 43 and Article 41 of 4AMLD.[131] The GDPR supports these restrictions, known as purpose limitation, in Article 5(1b) specifying that data cannot be processed in a way incompatible with the purposes for which it is collected.

For US FIs, there is no legal requirement to separate AML/CTF from commercial data use. FinCEN makes distinctions for AML/CTF data for the non-disclosure of SARs and data shared under § 314(b) among domestic financial institutions that can only use the data gathered from others for AML purposes, but does not seem to address its use internally to an institution or within a group. Therefore, US firms operating in the EU or dealing with European clients, must monitor their employee access and use.

One EU-based compliance officer stated that while there were policies in place barring marketing access, personal relationships within the firm meant that it was "fairly easy" to call an officer to gain the information they needed. IT experts questioned how one might engineer database structures to accommodate this requirement and how the financial services could separate the business from compliance completely. Data tagging (notations to alert FIs to possible data protection violations) is not enough, but pseudonymization might offer a solution. PII data should be restricted to compliance personnel and access to this data controlled through user-specific logins and technological means (e.g. access permissions, firewalls, or separate servers). As KYC data is collected for commercial and AML/CTF purposes, the duality of financial data, are the gravest technical and administrative challenges to implementing privacy in compliance.[132]

3.10: Enterprise (Group)-wide Sharing – SARs & Supporting Data

The conflict between US and EU views on enterprise-wide SAR and underlying data-sharing ranks among the greatest obstacles to implement a cohesive AML compliance strategy across an organization. Interviewees believed data-sharing constraints heightened the risks of doing business

and opened firms to regulatory scrutiny not only from data protection authorities, but from AML regulators who expected their programs to operate at enterprise levels. Data-sharing constraints curb an MFI's ability to follow the money and undermine the effectiveness of the FATF regime. When foreign branches, subsidiaries and affiliates cannot access and share enterprise data they cannot see client, transactional, or behavioral links across their businesses, which can create repetitive or incomplete reports to national authorities. Despite widespread industry perceptions that EU data protection requirements posed the greatest constraint to group-wide data-sharing, the research found that *both* US and EU laws impose legal controls that inhibit data flows.[133]

3.10a: Europe

4AMLD requires a group-wide AML program accompanied by a group-wide privacy program. Article 3 defines "group" as "a group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation…"[134] and requires all members of a group to participate in system-wide AML compliance that includes the sharing of SARs and underlying data. FIs are required to implement and train all staff on appropriate data protection procedures across the group. The Directive does not prevent disclosure with obliged entities and entities from third countries that are part of the group. As long as they are part of "the same professional category and are subject to obligations as regards professional secrecy and personal data protection" data-sharing is permitted.

In Article 39, 4AMLD prohibits disclosure to customers that "information is being, will be or has been transmitted" or that a "money laundering or terrorist financing analysis is being, or may be, carried out" which preserves the confidentially usually required of criminal and national security reporting and investigations. 95/46/EC protected the confidentiality of SARs and underlying data noting that "tipping off" individuals through notification or access is not allowed when data is processed in the "public interest" which includes ML and TF.[135] The AML Directive deals with the problem of SAR confidentially and an individual's right to access by allowing supervisory authorities, or the EDPS, to investigate the "lawfulness of the processing." 4AMLD gives little indication how Member States, or MFIs, might implement or enforce access requirements inside or outside the EU, but many European companies have policies and procedures for dealing with DPAs and these can be expanded to include compliance.

A 2009 European Commission study on AML compliance by cross-border banking groups examined how national laws under the 3rd Money Laundering Directive (3MLD) affected group-wide implementation for intra-EU multinationals. Since these same laws must accommodate 4AMLD's

group-wide requirements, it is worth noting its findings. EU AML prevention is based on the territoriality principle. FIs must comply with the Member State law where that office is located, which means that an MFI group can be subject to many national AML laws.[136] At the time of the study, 18 Member States required MFIs to assess AML prevention across their business lines and geographic locations. While this coincided with the Basel Committee's AML risk management standards (updated in 2014), the report noted that the territoriality-based AML regime maintained the Member State's regulatory power, which perpetuated policy and procedural variances across the group.[137] It is therefore not surprising that European firms preferred to conduct transaction monitoring locally and validate policies and procedures with the parent bank and avoid regulatory liabilities at the national level. Thus, despite 4AMLD's group-wide AML provisions, compliance operations will continue to be significantly influenced by local demands.

Inconsistencies among Member State AML/CTF are mirrored by 95/46/EC's equally territoriality-based national data protection. The GDPR will allow data-sharing among "a group of undertakings or institution affiliated to a central body," but the exceptions for defense and national security explained in Section 2.2b permit Member States to impose access limitations, set different standards for technical and administrative safeguards, and decide how stringent they will be in their enforcement. 4AMLD reinforces the GDPR's exceptions in Article 41,

> …adopt legislative measures restricting, in whole or in part, the data subject's right of access to personal data relating to him or her to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned to: (a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or (b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardized.

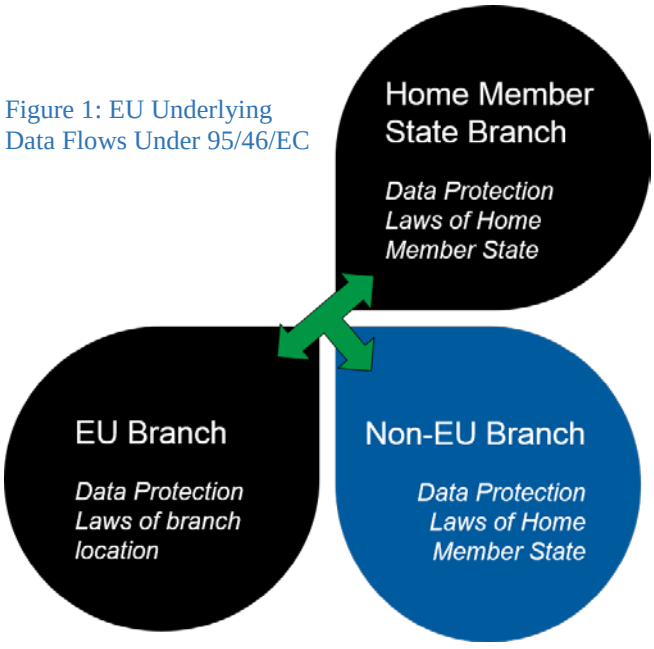


Figure 1: EU Underlying Data Flows Under 95/46/EC

At this time, it is too early to determine how the Member States may approach these issues or how it will affect the financial services. It is certain though that despite the EU's attempts to harmonize data protection, AML/CTF compliance will continue to deal with intra-EU data protection inconsistencies, which may resemble Figure 1. Nonetheless, the GDPR will heighten the EU's ability to *enforce* 4AMLD's data protection provisions inside the

EU, and for data flowing to third countries such as the US. 4AMLD stipulates that FIs must notify supervisory authorities (not defined as DPAs in the text) when operating in a country with inadequate privacy protections and put measures in place to "the extent the third country so allows." If authorities are unsatisfied with these actions they can impose penalties or request that the company cease operations in that state.

3.10b: The United States

Motivated by disclosure and confidentiality, the US restricts SARs and underlying data-sharing at home and abroad in some capacity. As illustrated in Figures 2 and 3, FinCEN does *not* allow US based multinational financial (depository) institutions to share SARs across the group.[138] Domestic FIs may share a SAR with head offices and controlling companies if they are domestic or foreign, but not with its foreign branches and affiliates. Regulations permit foreign branches to share SAR and underlying data only with its US head offices and controlling company.[139] Foreign branches, Edge and Agreement corporations, are not under BSA jurisdiction, but the law does require foreign branches to implement US-level AML systems and comply with local standards, although US authorities may not have the ability to do on-site inspections of foreign operations.[140]

In 2006, FinCEN recognized the need for head office involvement in SAR processes and allowed sharing from the bottom up only with confidentiality agreements in place,[141] but fell short of allowing SAR sharing to affiliates[142] in the US and abroad. This was remedied in 2010 as FinCEN and federal banking regulators recognized affiliates who were subject to SAR regulations.[143]

> … a depository institution that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate, as defined herein, provided the affiliate is subject to a SAR regulation. The sharing of SARs with such affiliates facilitates the identification of suspicious transactions taking place through the depository institution's affiliates that are subject to a SAR rule.

Figure 2: US Domestic SAR & Underlying Data-Sharing

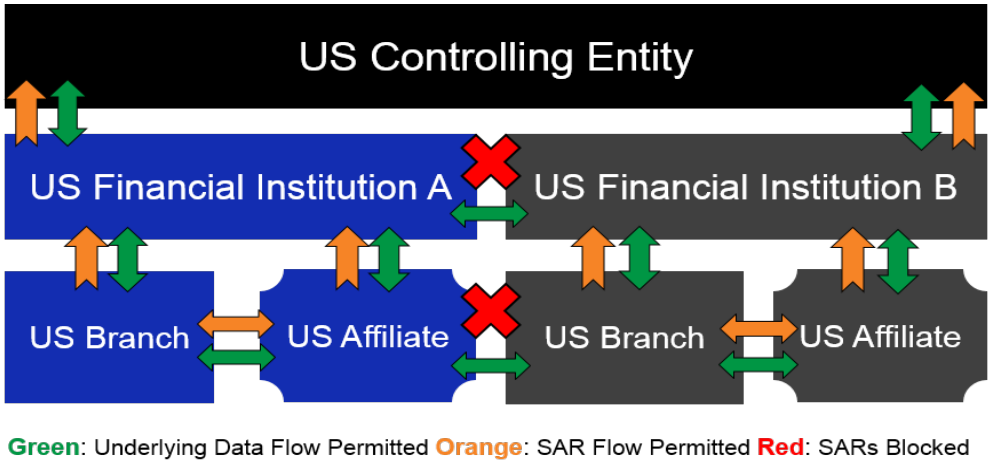


Figure 3: US International SAR Flows

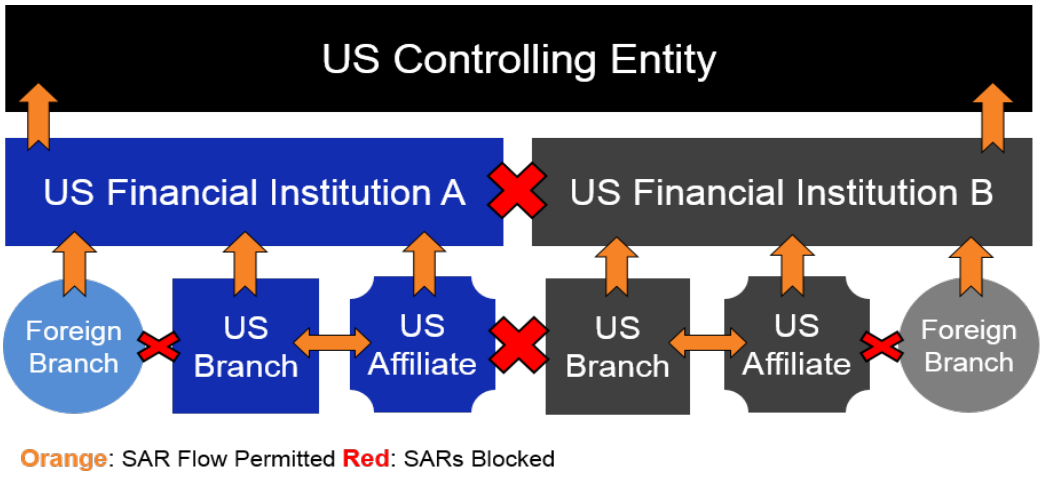
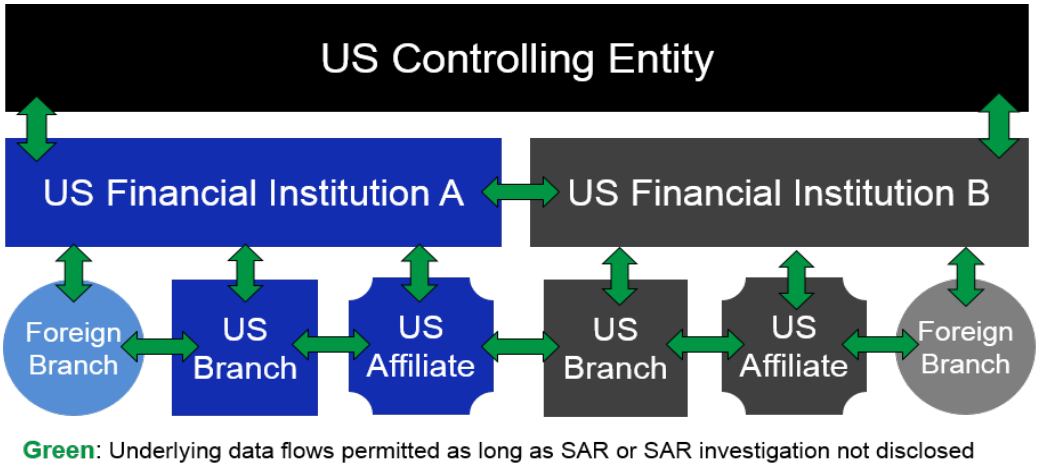


Figure 4: US International Underlying Data-Sharing



Yet, legal ambiguities remain. As foreign branches of US banks are affiliates, but not subject to BSA regulation they were omitted from these permissions. This has put US MFIs in difficult operational situations. The Clearing House LLC, a nonpartisan banking association, sought clarification on this point in March 2015;

> …a U.S. depository institution that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches. (Nor may it share such information with foreign affiliates for the same reason.) Moreover, the 2010 guidance prohibits an affiliate that has received a SAR from a depository institution from further sharing that SAR, or any information that would reveal the existence of that SAR, with an affiliate of its own (even if such second affiliate is subject to a U.S. SAR regulation). An important net effect of FinCEN's position in this regard is that the U.S. depository institutions of globally active banking enterprises may not share SAR information with foreign branches or foreign affiliates, nor may such information be disseminated within global banking enterprise by their parent companies.

Thus, the legal foundations concerning underlying information seem straightforward (Figure 4), but there are legal ambiguities. US FIs cannot disclose, acknowledge, or reveal the existence of a SAR, but they are not prohibited from disclosing underlying facts, transactions, or documents that have contributed to a SAR.[144] The Clearing House demonstrated that FinCEN's 2010 Final Rule omitted documents that "may identify suspicious activity but that do not reveal whether a SAR exists" from confidentiality restrictions, but later explained that confidentiality might be applicable "…in appropriate circumstances to material prepared by the financial institution as part of its process to detect and report suspicious activity…"[145]

The inability to share SARs and accompanying data with foreign branches of US institutions weakens the operational and organizational ability of US firms to implement group-wide AML/CTF compliance programs recommended by the FATF and the BCBS. MFIs who must build "artificial curtains" into their systems that raise costs, and leads to duplicative and confusing reporting lines where AML officers working for US banks in foreign branches must sanitize internal reports to avoid breaching US SAR confidentially rules. In some cases compliance officers must re-file US SARs with local regulatory authorities.

Interviewees believed that this is an "easy fix" since FinCEN could; 1) issue guidance to require confidentiality agreements with foreign branches like it does with US affiliates; and 2) recognize FATF compliant states as having adequate AML standards to ensure quality reporting within a group and with US standards. Where US authorities are concerned that foreign AML laws are not up to US standards, they could strengthen BSA enforcement procedures (already in place) that allow examiners to review overseas affiliate and branch policies and require additional measures – much like 4AMLD. The EU has acknowledged the US system as an adequate AML jurisdiction to

allow European firms to engage in group data sharing within the US, and the presence of data protection in 4AMLD might actually increase internal accountabilities for data collection, management, access, and use.[146] When one considers that challenges of harmonizing 28 European Member State policies to ease group-level data-sharing, the US's hesitancy to allow the practice, especially in light of the GDPR and 4AMLD exceptions, seem pale in comparison.

Several interviewees explained that US officials fear group-wide sharing with foreign branches might compromise SAR confidentiality. They also cited concerns about "reciprocity" among LEAs. Cooperative MOUs among US and EU FIUs, and the Umbrella Agreement will add an additional layer of data protection for inter-LEA transfers that will strengthen accountability and confidentiality, and make these arguments seem weak in the context of the transatlantic relationship. However, one US interviewee believed that EU banks used data protection as a shield against US-based civil prosecution of EU banks charged with conducting transactions.

3.10c: Cross-Institutional Data-Sharing: PATRIOT 314(b) & 4AMLD

4AMLD permits data-sharing between FIs and FI groups for AML/CTF purposes with adequate data protection measures in Recital 43 ("…while fully respecting fundamental rights…"), Articles 25 and 26, in the third party section the Directive explicitly authorizes "member organisations or federations of those obliged entities…" to share data, but only mentions CDD or record keeping, which paves the way for cooperative data-sharing arrangements among MFIs such as KYC Exchange Net AG, Markit Genpact KYC Services, and SWIFT's KYC registry.[147] FIs that are members of these arrangements are responsible for implementing national data protection laws that allow for the legal transfer of their data to these cooperatives. Typically, banks are responsible for assuring data transfers to registries are handled according to data protection standards. Data subject access requests are directed to the bank, not the registry management company. These federations are obligated to present data upon demand to authorities to "immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner."[148]

4AMLD specifies data-sharing in the context of CIP and CDD requirements or data-sharing within a group, but it does not include inter-institution AML data-sharing at the EU level. The US though, does encourage data-sharing among FIs beyond CIP and CDD data under PATRIOT § 314(b),[149] but it has had varying degrees of FI support like its § 314(a) counterpart. Section 314(b)

enables financial institutions and associations of financial institution to share AML/CTF information under a data-sharing safe harbor, so long as certain conditions are met. It is completely voluntary, and only applies to firms located in the US which are required "to establish and maintain an anti-money laundering program" so foreign branches or institutions are ineligible. FIs or associations apply for certification with FinCEN to announce their intent to engage in information sharing with other qualified entities. Certification involves a one-page form that provides the FI's name, address, primary regulatory body, and point of contact for the program, and an acknowledgement that data "will not be used or disclosed for any purpose other than as permitted."[150] FIs can verify that another FI is certified on its own or via a FinCEN published list accessible to § 314(b) members.

Although § 314(b) has the potential to promote cooperation across the industry, several interviewees noted that FIs avoid it because they did not want to share data with FIs whose AML compliance reputations were less than stellar, because they believed that other banks use it as a CDD "shortcut" rather than conduct their own due diligence, or they have simply not participated due to confusion about the data they could share without liability. 314(b) guidance cites that,

> …financial institutions or associations of financial institutions may share information with each other regarding individuals, entities, organizations, and countries for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering. …if sharing participants suspect that transactions may involve the proceeds of ***specified unlawful activities*** under money laundering statutes, information related to such transactions can be shared under protection of the 314(b) safe harbor.[151]
> ...however, that while information may be shared related to possible terrorist financing or money laundering that resulted in, or may result in, the filing of a SAR, Section 314(b) does not authorize a participating financial institution to share a SAR itself or to disclose the existence of a SAR.

Under these criteria, § 314(b) promotes inter-firm data-sharing beyond European practices since FIs can share *any kind* of data "possibly" relating to ML and TF, as long as they do not expose the existence of a SAR or share the SAR itself. However, because of the confusion over the legalities of sharing underlying data explained above, compliance professionals wondered how § 314(b) could possibly protect them from exposing an investigation or the presence of a SAR since "If you are asking and giving a lot of information on a subject that points to a SAR filing, then the person on the other side can figure it out."[152]

3.11: Third Countries with 'Inadequate' AML & Data Protection programs

Europe's group-wide AML and data protection requirements will impact all European and US firms in some capacity. Where EU based multinationals decide to engage in business in areas with inadequate AML/CTF regimes (e.g. on FATF's non-compliant or blacklist), companies with "branches or majority-owned subsidiaries located in third countries" are responsible for implementing AML programs and data protection "to the extent that the third country's law so allows."

It is the European private sector's decision whether to engage in high-risk markets, but it does so in a Catch-22 scenario since it must put in place AML *and* data protection policies and procedures to satisfy EU regulators. And they must do so with an eye towards their host country's laws that may conflict. 4AMLD seems to suggest an escape clause since financial institutions could claim they complied to the greatest extent *possible* under a third country's legal constraints. Still, MFIs are required to report any deficiencies, concerning AML and data protection, to Member State authorities who can require "additional measures." In the event authorities deem these insufficient they can "exercise additional supervisory actions, including requiring that the group does not establish or that it terminates business relationships, and does not undertake transactions and, where necessary, requesting the group to close down its operations in the third country."[153] The US is an adequate AML state, but not adequate in privacy. The GDPR holds firms accountable for any data transferred to a third country, including onward transfers of data, stipulating that they "only be carried out in full compliance" with the Regulation.[154]

It is unclear if or how data protection authorities would approach privacy enforcement of an FI's AML/CTF compliance practices. By making MFIs responsible for EU level AML and data protection across the group and in third countries with inadequate protections, the EU 1) uses the private sector as a vehicle to extend EU AML standards to non-compliant jurisdictions; 2) encourages EU MFIs to establish and comply with enterprise-wide AML and data sharing requirements and makes banks liable for their implementation outside the EU; and 3) extends the EU's power over data protection rules outside its borders.

US banks are allowed to do business in non-AML compliant states, as long as those states are not on the FATF High-Risk and Non-Cooperative Jurisdictions list, or US and United Nations sanctions lists.[155] FIs must implement US level AML programs and comply with local regulations.[156] PATRIOT Section § 312[157] and 31 CFR § 1010.610(a) require US banks to take EDD measures when

operating in FATF deficient states or with PEPs in certain jurisdictions, including correspondent relationships and foreign clients with accounts in the US. US-based authorities are authorized to check that the head office has developed AML systems and audits for their foreign presences as if they were applicable under BSA, but has little direct control to do on-sight regulatory visits at the foreign branch. In essence, US law treats all foreign branches, affiliates and subsidiaries as inadequate because there are no protections for US banks doing business abroad for compliance. Of course, US firms are not required by US law to consider the privacy laws of other states in their AML/CTF operations.

US sanctions only apply to US persons, and foreign owners and siblings are not technically subject to them, but if they engage in transactions through, or otherwise use the services of, US subsidiaries or siblings, then US sanctions do apply. For example, PATRIOT § 311 authorizes the Secretary of the Treasury to impose "special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of primary money laundering concern." The most serious measure blocks foreign banks from accessing dollar markets, and is considered a "death sentence" for FIs that depend on correspondent banking in the US.[158] There is some criticism that the US government uses § 311 to extend its territorial reach, but it has used other means to penalize foreign banks for doing business with restricted groups. In 2014, the Justice Department fined BNP Paribas $8.9 billion for violating the International Economic Powers Act and the Trading with the Enemy Act for moving dollar transactions through its New York office with blacklisted Sudanese companies.[159] Some foreign banks have voluntarily adopted US sanctions compliance across their global enterprise out of an abundance of caution or as an "act of contrition" after enforcement actions.

4. THE GDPR: PROFILING, AUTOMATED PROCESSING, RBA & DE-RISKING[160]

The high volume of data processing involved in the business of finance requires automated or semi-automated systems and software that make data collection, maintenance, and analysis efficient and accurate.[161] Constant monitoring and profiling sits at the core of AML/CTF and the prevalent use of computer-aided decision-making within these processes necessitates an examination of their data protection implications.[162] This is relevant since the GDPR specifically addresses profiling and automated processing, while there is no comprehensive law that covers these practices in the US.

4AMLD uses the word profile in Recital 31 and Article 13, requiring FIs to construct an "identity and business profile" for all customers. The Directive does not define what constitutes a

profile. And while it does not use the words automated or semi-automated, it does refer to "monitoring" in Recitals 7 and 43, and Articles 12, 13, 15, 18, and 20, thereby eschewing identification or preference of the methods FIs might use to monitor.[163] For example, Article 13 mandates continual observation of customers by,

> (d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

This is also true in the US. FinCEN requires monitoring at many points in the client relationship and FIs have developed several schemas to target various levels of business – transactions, accounts, household, and geographic – depending on the FI's compliance program. And, after filing a SAR, banks continue to monitor the customer for at least 90 days.[164]

In their reviews of 4AMLD's drafts, the EDPS and WP29 expressed deep concern for AML/CTF "profiling techniques under CDD obligations" which they felt were "opaque" and "operated without a clear legal basis." They noted the difference between the analysis of KYC data for identification purposes and "subjective or sensitive information linked to profiling data." These and other factors necessitated their recommendation for legally-mandated Member State-led safeguards for profiling operations since FIs cannot solely depend on the free consent of the client. Yet, their concerns went beyond fundamental rights and freedoms. WP29 understood profiling's limitations and desired to curb the negative results from profiling and automated decision-making that affected individuals *and* the quality of data FIs deliver authorities.[165] In one example WP29 noted the dangers of monitoring software failures that undercut value of AML/CTF,

> The "base-rate fallacy" (lack of accuracy) shown by the number of false positives or false negatives. Profiling using false positives means that attributes are (or could be interpreted to be) highly likely to result in non-money launderers and non-terrorists being prevented from accessing financial services, whilst "negative positives" mean there is no absolute guarantee that all money launderers and terrorists will be intercepted, a.o. due to the adaptive behavior of real suspects.

Because of these issues, EU data protection authorities asserted that profiling using automated or semi-automated methods *should only be permissible in exceptional cases*.

Monitoring occurs at all stages of the business relationship, so this would be impossible to apply in practice. FIs profile individuals, entities, and markets, to assess them as customers or potential customers. Thereafter, firms continuously monitor client transactions and evaluate their behaviors to provide better services, and to inform decisions on AML/CTF investigations and

reporting. The extent that humans investigate suspicious persons or events varies with the compliance department, but the industry agrees that the human element and employee training and education is crucial (and costly).[166]

The industry invests billions into monitoring software that performs several functions: 1) transaction monitoring (to determine a customer's activity); 2) behavior monitoring (comparing a customer's financial and non-financial details to predict activity) that continuously validate someone's identity to protect the FI's reputation and protect customers from and fraud; 3) filtering clients and screening transactions against sanction and terrorist lists; risk scoring to identify and prioritize risks across the business; and 4) PEP EDD monitoring.[167] Other software (sometimes integrated with above) assists compliance officers with reporting to reduce errors, speeds up the investigation process, creates work logs to track actions, and validates reports. All of these systems' methodologies (red flags, thresholds,[168] automatic learning algorithms,[169] etc.) must be constantly audited to maintain accuracy and updated to integrate new ML and TF methods. Like KYC databases, the accuracies of these systems depend on the quality of their algorithms and the data supporting them.[170]

95/46/EC did not explicitly mention profiling, but Article 15 did refer to "data processed by automated means,"[171] and most Member States transposed these protections into their national laws.[172] The Directive did not provide a general right for data subjects to object to the processing of their data via automation, but subjects could raise objection on "compelling legitimate grounds."[173] Instead, Article 12(a) granted individuals the right to have "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions…" Article 15's guidance on "automated individual decisions" stated that these rights apply whenever a person is subject to "legal effects" of a decision by automated processing. The Article allowed automated processing "authorized by a law" but also required Member States to impose "safeguards" to balance the needs of national security and criminal investigations with the fundamental freedoms of individuals. It did not offer guidance on how to legislate safeguards.[174]

The GDPR *does* deal with profiling and computer-aided processing so there are incentives (via weighty fines or reputational-driven reasons) for the financial services to give serious attention to the subject.[175] Article 4(3aa) defines profiling as

> any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

In Article 2 the Regulation refers to automatic-processing as it "applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[176] An individual's rights in profiling and automated decision-making are enumerated in Articles 19 and 20.[177] Article 19 states that the data subject has the right to object,

> the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on these provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

AML/CTF fell under compelling legitimate grounds, but Article 19's reference to Article 6 (e) and (f) gives individuals the right to object even in cases where automatic processing is done for legitimate reasons.

> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance exercise of their tasks.

As the following analysis explains, it is unclear how or when data subject would be able to object to AML/CTF processing. The GDPR's allowances and exceptions make differentiating between a data subject's rights and the realities of compliance practices rather confusing.

Regardless, data subjects have the right to understand how their data is used. Recital 48 gives data subjects the right to be informed "about the existence of profiling, and the consequences of such profiling" and Article 14(h) further designates that firms provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[178] These notifications mean to inform people about the aforementioned opaque methods that banks use to process their data and correct "knowledge asymmetries" that may bar EU citizens from exercising their fundamental rights. When individuals are unaware of how financial institutions utilize their data, do not understand the complexities of their profiling processes and techniques, or do not understand how personal actions contribute to decision-making, then they have no means of challenging the means or the results.[179]

Article 20 "Automated individual decision making, including profiling"[180] provides exceptions for AML/CTF, while reinforcing the use of processing safeguards and the right of data

subjects to challenge legal outcomes. Paragraph 1 gives the data subject the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Yet, 1(a) exempts any decision "necessary for entering into, or performance of, a contract" and 1(b) exempts cases "authorized by Union or Member State law…which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." Article 21 reinforces these exceptions and permits Member State derogations in profiling and automated methods used for national security, defence, public security, "prevention, investigation, detection or prosecution of criminal offenses…or prevention of threats to public security," and "monitoring, inspection or regulatory function" relating to the above.[181] These passages retain some of 95/46/EC's exemptions, but in each case the GDPR stipulates that Member States must adopt legal safeguards for these cases. When profiling is done for the performance of a contract or through explicit consent, controllers must implement "suitable measures" to safeguard the data subject's rights including the "right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[182] The main concern seems to center on how profiling affects data subjects when it *produces a legal outcome*.[183]

Thus, individuals should be notified of profiling techniques and how their data is processed with automated or semi-automated means. At some point they can object to the processing if it is not done in line with safeguards, but 4AMLD restricts individuals from challenging the process or the results of compliance monitoring directly, instead allowing supervisory authorities to determine the legality of processing by the request of the data subject. It is unclear how authorities would do so or how anyone would be alerted that they were the subject of a SAR investigation since they are confidential. Presumably, the only way a data subject would be made aware of the legal outcomes of an investigation is if they were the subject of some legal action (subpoena, arrest, indictment, etc.).

At each point in the process, the GDPR makes it clear that profiling *can* be done, *but only if the necessary safeguards have been applied.* So what do safeguards look like? The criteria are broad. Legislation must clarify the purposes of processing, data categories, the scope of restrictions, safeguards to "prevent abuse or unlawful access or transfer," "specification of the controller or categories of controllers," retention periods, risks to data subject rights, and the right of data subjects to be informed of these restrictions.[184]

Recital 75 lets FIs know that they are responsible for these safeguards, and other measures, in their profiling and automated operations. A Data Protection Officer (DPO) is mandatory when "processing is carried out by a controller whose core activities consist of processing operation that require regular and systematic monitoring of the data subjects, a person with expert knowledge of

data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation." Article 33(2) requires that firms conduct data impact assessments on whenever there is "systematic and extensive" evaluations of individuals based on automated processing that produces legal effects. With systemic monitoring or processing that concerns "data relating to criminal convictions and offenses" Article 35 requires FIs to employ a DPO, who can be someone already employed with the company. This is reinforced by Articles 36 and 37 which outlines a DPO's duties within a firm to include monitoring compliance, "awareness and training," conducting audits, "provide advice" for impact assessments taking account of the "risks associated with the processing operations" and serve as the contact for data subjects and supervisory authorities.[185]

AML/CTF's blanket privacy derogations may be a thing of the past, and if the Profiling Project's 2014 findings are any indication, the future of EU Member State safeguards and enforcement on profiling will be a rocky one. A survey of DPAs revealed that officials saw profiling in the financial services, including AML/CTF compliance, as the highest threat to an individual's fundamental rights and freedoms.[186] In 2010, the Council of Europe tried to fill the legal and definitional gap left by 94/46/EC on profiling and offered recommendations on the aforementioned safeguards, but few Member States have adopted them.[187]

4.1: RBA & De-Risking

The US and EU have chosen the RBA method because "banks know their businesses best" and as FIs collect and analyze commercial data on a daily basis they are suited to recognize illicit activity in the financial system. The RBA method therefore requires that banks process enormous amounts of data to guide their decision-making during every step of their businesses, which is supported by profiling and automated processing.

However, there has been significant debate about RBA's viability to identify ML or TF offenders to the satisfaction of regulatory authorities.[188] First, the subjectivity of compliance and the ever-evolving methods employed by criminal and terrorist financing force FIs to constantly adjust their routines causing firms to constantly invest in software solutions and additional employee training. Second, these conditions have created uncertain foundations for compliance assessment, which according to many interviewees, have "made it nearly impossible" to meet the expectations of authorities without courting fines and litigation. Regulators themselves admit that it is difficult to set standards because of the factors unique to each product line, client, and jurisdiction, and the fluidity of methods used in the illicit economy and terrorist finance.[189]

The GDPR's focus on profiling and computer-aided decision-making holds wide-ranging implications for RBA that have led to de-risking. De-risking is a consequence of profiling, but it also arose from the difficulties involved in setting, and executing, RBA regulatory standards. RBA facilitates creating a profile of an individual or in some cases, a market,[190] to inform decision-making on a host of factors and data points so an FI can decide whether to accept or reject a client. The intent of RBA to *inform* the AML/CTF controls that a bank puts in place for a client/potential client relationship, based on the bank's risk assessment of the client. According to regulators, banks should reject or exit a client relationship only in rare instances when a FI believes it *cannot adequately control* the AML/CTF risk.

Banks claim that they rarely de-risk due to the actual AML/CTF risk of a client. Instead, de-risking occurs due to the regulatory pressure, or the cost of "proving" their RBA is effective. While many compliance professionals agree that de-risking occurs, they stipulate that the degree to which it happens depends upon the institution's compliance measures. Some insist that de-risking is used to *manage* risk, and banks will accept higher risk customers with higher fees to cover the costs of doing business rather than deny services.[j]

The fear of fines and (perhaps more so) reputational damage drives compliance, and de-risking has affected consumer relationships and services.[191] FIs assure that their risk assessments do not result in what the FATF calls the "wholesale" removal of individuals or markets from access to the formal banking system.[192] There is evidence that MFIs are cutting off legitimate customers such as users of virtual currency, marijuana businesses, pawnbrokers, the porn industry, correspondent banking, cash intensive businesses, non-profit organizations, and weak government, high conflict areas in across the globe.[193]

Privacy advocates worry that group-wide data sharing may spur de-risking prompting MFIs to create blacklists.[194] In the US, banks have utilized similar methods to detect fraud[195] like the Early Warning and ChexSystems services that maintain lists of customer's checking account transgression, or the FTC's Sentinel database that tracks fraud cases. These issues have led to dialogs about the "collateral effects" of de-risking and how to safely embrace these marginalized individuals and groups in the formal banking system.[196] The GDPR's fears about the "legal effects" of profiling apply here. While the US does not have a comprehensive law for financial profiling, several pieces of legislation do tackle specific areas where the practice results in discriminatory decisions, like denying credit or employment based on inaccurate data or judging persons based on race, creed, ethnicity, or gender.

[j] Some FIs manage risk by being overzealous in their reporting. The practice of filing to prevent regulatory risk is called a "defensive" SAR which can dilute the value of data delivered to authorities.

But the negative consequences of de-risking are not limited to the business of banking. As FIs withdraw from these clients and markets for whatever reasons, they undercut the state's ability to gather data and employ Information Statecraft. Services such as money changing, cash-based, gift cards, used frequently in countries with unstable governments, those experiencing war or conflict, areas with unbanked and underbanked populations, or high mobile device banking, are difficult to regulate, carry high risks which incur costs for banks, and can be magnets for illegal activities. Regulatory risks incentivize banks to disengage from the very areas and populations where governments seek actionable data to combat ML and TF. When MFIs avoid these markets, authorities have less chance of garnering actionable intelligence.[197]

5. CONCLUSIONS

Information Statecraft: Data Ownership & Financial Institutions

It would not be a stretch to say that the financial services occupy an indispensable role in the state's ability to successfully employ Information Statecraft. However, legal disconnections between US and EU AML/CTF and privacy laws challenge the ability of multinational financial institutions to implement consistent policies and procedures across their business and jurisdictions that inhibit a state's ability to gather data to track illicit economy and map networks of political violence.

The implementation of data protection in AML/CTF compliance is in its infancy, and there are deep educational and informational divisions among the privacy and AML/CTF sectors. Individuals working in the financial services who were versed in both arenas are rare;[198] consultancies and vendors have yet to combine AML/CTF and privacy services for their clients and typically offer privacy as a supplementary or "on-demand" amenity. Unfortunately, the same divisions are present on the government legislative and regulatory sides with privacy and AML/CTF experts crafting laws reflecting their own interests and expertise with consultation, but not enough cooperation.

Although this research demonstrated obstacles from both the US and EU perspectives, the Europeans are setting the terms of this relationship. The EU's inclusion of data protection into the AML/CTF security atmosphere will require the combined efforts of lawmakers, regulatory authorities, and the financial services industry to tackle financial data's legal and operational duality successfully. Even in 2013, the EDPS understood this dichotomy declaring "…the collection of data for anti-money laundering purposes takes place at the same time as the collection of data for commercial purposes." Throughout this research, financial leaders have asked, "Where do the

commercial functions of data end and AML/CTF functions begin?" and "Why should I care about data protection?" In lieu of legal guidance, the responsibilities fall on multinational corporations.

First, privacy suffers from an image problem in AML/CTF compliance. The EDPS and WP29 have repeatedly stated that privacy should be included in a positive way that is complementary to AML/CTF operations, not presented as a burdensome regulatory addendum. Unfortunately, legislation has failed to create formal cooperative mechanisms among AML/CTF and privacy officials, and one finds the disconnection between the two fields trickles at the corporate and professional levels.[199] Privacy advocates try to appeal to businesses through legal and ethical means, arguing that the private sector should be concerned about the abuse and misuse of data that threatens individual freedoms. These *are* salient issues in a digital society and the law must seek to protect these rights – human or civil. However, what is often absent from these dialogues is the positive discussion of privacy's value to improve AML/CTF compliance *and* profits. Privacy must appeal to business, be couched within operations, have a utility to the industry, and function as a valued commodity for its clientele.

This is an easier sell than most might think. Data privacy, whether in the US or EU model, helps businesses in all these aspects. Unfortunately, privacy and compliance professionals rarely occupy the same spaces to examine their overlap or compare notes. Even so, surveys and reports sponsored by their respective associations and services show they share the same anxieties about costs, fines, litigation, and reputational damage, and they discuss them in remarkably similar language.[200]

Both regimes place the burdens of cost upon financial institutions, and expenditures are rising. KPMG's annual global survey found that AML/CTF costs have risen between 45-53% over the past decade, which was supported by an ACAMS/Dow Jones study that projected increased workloads to incorporate new regulatory requirements in the coming years.[201] An IAPP/EY 2015 report showed privacy budgets rising too with 1/3 of respondents expecting growth for 2016. Financial privacy professionals reported strong expectations for professional opportunities – 68% in regulatory compliance and 46% for risk management, but seemed to share AML's negative view of privacy's profit utility; only 22% thought it aided revenue.[202]

Data privacy is not a supplement to AML/CTF, it is an enhancement. As AML/CTF regulators push a culture of compliance (through fines and other actions) and focus on individual responsibility, a good privacy program provides a trail of accountability at every stage of the process. Like AML/CTF, privacy forces companies to assess, classify, and understand their information flows and manage them through administrative, organizational, and technical means. These controls go beyond the IT aspects of information security; they help team members understand where the data is,

who has access to it, and how it is used, which can increase accuracy and efficiency in AML/CTF operations and beyond. This ultimately protects individuals and firms, and produces a more accurate picture of where to draw the line between compliance and commercial data usages, and how they may be able to neutralize personal data for marketing use.

The fear of regulatory risk and its ability to trigger reputational or brand damage dominates the narrative. KPMG's survey found that reputation protection drove compliance investments and involvement from the highest levels of leadership. IAPP/EY findings reflected these feelings demonstrating that reputational concerns dominate banking, but at the same time showed that privacy practices were "less robust" in finance compared to sectors that were "less regulated." Yet, financial privacy professionals thought programs aided corporate citizenship (56%) and reduced litigation risk (53%).[203]

Privacy procedures aid regulatory accountability, and they address public attitudes about privacy that go *beyond* breaches. Regulators have relied on the stick, rather than the carrot, to bring the private sector in line with the privacy and AML/CTF arenas, and this has produced an atmosphere of fear and distrust among officials and the public. FIs fear regulatory scrutiny which produces media headlines, triggers negative public perceptions, and ultimately results in reputational damage.[204] Public polls consistently rank the financial sector among the least trustworthy industries for privacy and data security. The general population has little faith in FI abilities to keep their data safe and frown on the practice of using or selling personal data for corporate profit.[205] Firms worry about data breaches and negative headlines that hurt their profits, yet they see data privacy as a special service and ignore public apprehensions about their business models. As the IAPP/EY report summarized, "Privacy underlies consumer trust and expectations. It draws on professionals' ethics and communications skills to identify the fault lines between new technologies and existing social values."[206]

In short, finance must overcome the view that they are entitled to client data. For an industry that already suffers from a less than favorable public image, especially in the wake of the 2008 financial crisis, this thinking must change even when that collection is mandated by national security concerns. EU interviewees were concerned about data use restrictions but accustomed to privacy requirements, still felt that protecting data was important, and believed that they could work with or around them. US interviewees were split on the subject, some tended to view data privacy as another regulatory burden upon their businesses, or a type of trade protection, while others thought they were already adequately regulated in this regard. Extreme views fail to take into account the shift in the transatlantic public's mood regarding corporate compliance in national security issues, the value that consumers place on their data, and their business relationship expectations. Companies that market

data privacy, and transparency, as a core service will gain consumer trust and profits no matter where they operate.

Next Steps & Opportunities: Member State Safeguards & Codes of Conduct

Despite privacy's image problem, there were members of the financial community who supported data privacy in AML/CTF. However, both backers and detractors agreed that there is very little legal or regulatory guidance to help them navigate these obligations. FIs worry that they will be trying to comply with another set of ill-defined and shifting standards in an AML/CTF compliance atmosphere that is already difficult to navigate. The legal conflicts with privacy do seem to make it nearly impossible for the financial services to implement one set of requirements without courting the ire of another set of regulators. It is therefore little surprise that the banking industry sees AML/CTF privacy requirements as among the most challenging regulatory requirements on the horizon.

The path forward may already be within 4AMLD and the GDPR through technical and organizational "safeguards." 4AMLD gives little guidance to FIs to determine their data protection duties in the context of its AML obligations, but it obligates FIs to apply these safeguards, although it does not define them. The GDPR does provide an outline in Article 21, but ultimately leaves the safeguards' legal articulations to national law. Thus, Europe's privacy diversity will continue for AML/CTF functions since 4AMLD allows national governments to exercise limitations on AML/CTF data protection, and the GDPR makes Member States responsible for the application of technical and organizational safeguards that will determine degrees of enforcement.

Still, because of Member States have yet to write safeguard criteria, the *next two years are critical* if MFIs wish to contribute to data protection standards that fit their transnational AML/CTF operations. If the financial services are looking for an invitation to contribute and collaborate, they have it. The GDPR formally calls for cooperation among industry associations to formulate "codes of conduct" in Recital 76 and 76a to set the technical and organizational standards outlined in the Regulation. Article 38 outlines the codes' provisions, which are broad enough to accommodate compliance's risk-based regime, including secure systems and fair and transparent data processing for legitimate interests. This is a prime opportunity for the industry to contribute to the dialogue and the Member State safeguards that will impact all aspects of their compliance operations.

This will require frequent government/regulatory and industry interactions. AML/CTF regulators and DPAs should meet regularly and work with financial institutions. Financial industry representatives can help set safeguards that ensure compliance with both legal regimes. It is likely

that cooperation among these groups will be difficult. They are accustomed to cautious consultation, but rarely engage in collaboration due to an unfortunate atmosphere of distrust.[207] Business leaders expressed feeling constrained to speak freely among officials. As one explained, "Not every suggestion we make should be treated with suspicion. There are genuine concerns and experience we bring to the table that are relevant and should be taken seriously." There was, however, also acknowledgement that the industry contributed to this air of distrust owing to its past mistakes. On the other side, regulators conveyed exasperation at these comments believing that they had done everything to accommodate industry concerns. Furthermore, mitigating the security-privacy conundrum will depend on the private sector's ability to overcome a culture where protecting a competitive edge can often overshadow the common good.[208]

These public-private discussions need to reflect financial data's transnational nature. The EU is setting the terms for AML/CTF data protection because the US does not have a comprehensive privacy regime or require privacy's inclusion into compliance. However, a European-centered effort will invariably cause friction with US practices regarding data transfers to authorities, rights of redress, and American concerns about nondisclosure, and its sensitivities over maintaining SAR and underlying data confidentiality. Codes of conduct and safeguards should be formulated with multinational data flows in mind, which would help address the cross-national issues flagged in this paper.[209] Flexibility is crucial due to the differences in US-EU privacy views, because money launderers and terrorist organizations change their methods, and because these practices will shift in accordance with the FI's risk profile.

Financial Institution Preparations

Until these safeguards are established, financial institutions should already be taking inventories of what data they have, where it comes from and where it resides (geographically and technically – cloud or legacy systems, and through vendors), where it flows, who accesses it, and for what reasons. Furthermore, they should acknowledge that like the legal and regulatory divisions chronicled in this paper, the same educational and informational stove-piping is prevalent in the privacy and compliance professions - and within their own corporate structures. While AML/CTF and privacy professionals recognize the need for more regulatory and industry collaboration in setting standards of data collection and analysis, these cooperatives are rare, and there are few individuals who understand them equally or able to communicate across them.

To tear down disciplinary barriers, organizations should; a) create integrated compliance teams with AML/CTF, privacy, and information technology (IT) experts[210] within matrix decision-making environments; or b) create positions specifically tasked with communicating and

coordinating across these areas of expertise and incentivize privacy, IT, and compliance employees to seek cross-training and certifications. Professional associations and consultancies should offer integrative AML/CTF and privacy services to smaller firms so they are cost effective.[211]

Either of these methods will build teams that can understand financial data's commercial and national security duality and help their organizations identify their regulatory exposures. These individuals or teams will help FIs produce a map of enterprise-wide risk assessments that take legal, technical, and operational areas into account for AML/CTF and privacy. And it will make it easier for firms to apply safeguards because they will have people and systems in place that understand them.

Finally, governments could encourage an understanding of end user views (FIUs, LEAs, Intel) and better AML reporting by monetarily incentivizing financial institutions to train their compliance officers in investigative intelligence techniques (there is a shortage of former LEAs and intelligence officials who bring that knowledge back to the private sphere). The same incentives should apply to privacy and IT professionals who are able to provide cross disciplinary perspectives.[212]

The confidential nature of AML/CTF reporting and investigations will always be in some ways at odds with privacy. But the financial services, and state officials should view these uncertainties as opportunities for public-private dialogues to set workable privacy standards within AML/CTF operations that will benefit financial institutions, states, and individuals.[213]

6. GLOSSARY

4AMLD	4th Anti-Money Laundering Directive
AML	Anti-Money Laundering
BCR	Binding Corporate Rules
BO	Beneficial Owner
BSA	Bank Secrecy Act of 1970
CDD	Customer Due Diligence
CIP	Customer Identification Program
CTF	Counter-Terrorism Finance
DPA	Data Protection Authority
EDD	Enhanced Due Diligence
EDPS	European Data Protection Supervisor
FATF	Financial Action Task Force
FCRA	Fair Credit Reporting Act of 1970
FI	Financial Institution
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GLBA	Gramm-Leech-Bliley Act of 1999
IT	Information Technology
KYC	Know-Your-Customer
LEA	Law Enforcement Agency
MFI	Multinational Financial Institution
ML	Money Laundering
MOU	Memorandum of Understanding
PEP	Politically Exposed Person
PII	Personally Identifiable Information
RBA	Risk-Based Approach
SA	Supervisory Authority
SAR	Suspicious Activities Report
SCC	Standard Contractual Clause
STR	Suspicious Transaction Report
TF	Terrorism Financing
WP29	Working Party 29

[1] For Information Statecraft see Frasher 2012 and 2013b, Frasher and Selmier 2013a, 2013b, and 2016.
[2] Kuner 2011 and 2013.
[3] The cultural concepts of privacy and data protection will be addressed in a large volume. The legal and compliance oriented analysis here focuses on information privacy law - rules that govern the "collection and handing of personal information." Swire and Ahmad 2012: 2.
[4] See Symantec 2015 survey regarding European public views on privacy.
[5] Whitman 2004.
[6] Coors 2010; and O'Cinneide et. al. 2006.
[7] See González Fuster 2014; and Bennett and Raab 2003.
[8] See 95/46/EC Recitals 30, 32, 34, 35, 36, 45, and 58. Sections II and III, including Article 26 on derogations.
[9] See Noonan and Brunsden 2015.
[10] See Moerel 2011; and Spies 2011.
[11] GDPR Recitals 19, 20, 21, and 22, pp. 14-15. Article 3 (Territorial scope) (1) "regardless of whether the processing takes place in the Union or not," (2) processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union."
[12] GDPR Article 24.
[13] GDPR Article 4 (5) and (6). Article 7 for the conditions of consent.
[14] GDPR Article 22 (controllers) and Article 26 (processors).
[15] GDPR Recitals 58, 61, 63a, 125, Articles 4, 5, 22, 23, 26, 28, 30, 32, 79 and 83.
[16] GDPR Article 38. See Articles 39 and 39(a) for certification.
[17] GDPR Article 6 and 6(3) for processing set by Member State law.
[18] GDPR Article 30.
[19] GDPR Article 41.
[20] 95/46/EC Article 13; and GDPR Article 21.
[21] GDPR Article 21 (2).
[22] GDPR Article 44. The Regulation permits transfers in cases of "explicit" and "freely given" consent, for the "performance of a contract," and when "legally required on important public interest grounds," but data subjects must be informed of the transfer risks to countries without adequacy. Articles 40, 41, and 42, the GDPR necessitates that all controller and processor third country transfers have "appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies."
[23] European Digital Rights, (n.d) believed it gave a blanket allowance for transfers from private companies to law enforcement authorities in third countries with inadequate protections.
[24] GDPR Articles 42 and 43.
[25] BCR-Ps were controversial. See WP29 2013c and 2014a.
[26] GDPR Article 42.
[27] For US attitudes on privacy see Pew Research Center, 2015 and TRUSTe, 2015. Turow, Hennessy, and Draper 2015 provide critical analysis of data in marketing.
[28] Whitman 2004.
[29] See Bloustein 1964; Simmel 1968; Reiman 1974; and Schoeman 1992.
[30] US FIPs influenced the OECD and Council of Europe's work. See US Secretary of Secretary of Health, Education, and Welfare Advisory Committee on Automated Personal Data Systems, 1973.
[31] See Meyer v. Nebraska (1923); Griswold v. Connecticut (1965); Stanley v. Georgia (1969); Ravin v. State (1975); Kelley v. Johnson (1976); Moore v. East Cleveland (1977); Cruzan v. Missouri Department of Health (1990); Lawrence v. Texas (2003).
[32] Swire and Ahmad 2012: 33.
[33] The applicable regulatory authority depends on the FI's function. They include: Federal Trade Commission (FTC), Federal Reserve (FED), Consumer Finance Protection Bureau (CFPB), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Commodity Futures Trading Commission (CFTC), Securities & Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB), The Office of Thrift Supervision, and National Credit Union Administration (NCUA). The States Attorney's General may also be involved.
[34] Carnor et. al. (5) recognized how the law could confuse "opt out" provisions noting, "GLBA's Financial Privacy Rule applies to the sharing of consumer financial information with non-affiliates, the FCRA restricts sharing consumer report information between affiliated companies, and FACTA limits when consumer report information shared between affiliates may be used for marketing." See 15 U.S.C. § 1681a(d)(2)(A)(iii), 15 U.S. Code § 6802 - Obligations with respect to disclosures of personal information, and "Affiliate Marketing Rule," prohibits companies that receive information that would be considered a consumer report if not for § 1681a(d)(2)(A)(iii) from using that information for marketing unless the consumer is given notice and the opportunity to opt out in 15 U.S.C. § 1681s-3(a)).

[35] See National Conference of State Legislatures 2015. For example, California's SB-1 or the Financial Information Privacy Act expands GLBA protections and requires written opt-in consent for financial institutions to share personally identifiable information (PII) with nonaffiliated third parties and they can opt-out of information sharing between FIs and nonaffiliated businesses. See Leland, Chan (n.d.) SB-1 and FCRA have a history of court battles. See Wilmer Hale 2008.
[36]Baker and Hostetler, Data Breach Charts; and Cranor et. al, 2014: 11.
[37] See FCRA 15 USC §§ 1681b, 1681u, 1681v, Dodd-Frank 12 USC § 5468, GLB, 15 USC § 6802 and RFPA 12 USC §§ 3412 and 3420.
[38] White House 2012; and Consumer Privacy Bill of Rights 2015.
[39] See Cranor et. al. 2014.
[40] Pillsbury-Protiviti noted in 2009 17 US States have enacted such laws: 37.
[41] See FTC "Consumer Sentinel Network Data Contributors." For Red Flags Rules 12 §§ CFR 41, 222, 334, 364, 717, 571 and 16 CFR § 681.
[42] FTC, 16 CFR §§ 680 and 698.
[43] Author interviews, European Commission February and March 2014. Sammin 2004; and Farrell 2002.
[44] Frasher, 2013a.
[45] Cranor, et. al. 2014; and FTC GLBA Guidance 2002.
[46] Sousa de Jesus 2004.
[47] See Schriver 2002; and Connolly 2008.
[48] European Commission 2013a and 2013b.
[49] The Judicial Redress Act has been tied to the Umbrella Agreement as part of Europe's efforts to extend data privacy rights to public authority data transfers, but it was initially introduced by the technology industry, as part of the Safe Harbor compromises. Interviews with US officials, September 2014 and April 2015.
[50] EUCJ 2015; Scott 2015; and Europe v. Facebook Prep Document 2015.
[51] Swire 2015; and Wolf and Maxwell 2015. The EP acknowledged Member State issues (2014). Thanks to Marieke de Goede for bringing this to my attention. Sidley Austin LLC (2016) produced an excellent analysis of the Schrems case and compared EU Member State laws to US federal laws for LEA and intelligence agency data acquisition.
[52] US Department of Commerce 2016 and European Commission 2016.
[53] FATF 2012. FATF Initially set 40 Recommendations to cover AML measures and added 9 after the 9/11 attacks to encompass terrorist financing. These 9 were absorbed into the original 40.
[54] BSA Statues: 31 USC §§ 5311-5314, 5316-5532, 12 USC §§ 1829, 1951-1959, Title 18 USC, Crimes and Criminal Procedure, and 31 CFR Chapter X.
[55] FATF 2014a: 6.
[56] Risk is a broad term used throughout the AML/CTF process. It may describe the greater scheme of RBA via 1) inherent risks (if no actions are taken); 2) control risks (a bank process designed to mitigate a type of risk); and 3) residual risks (risks after all controls have been applied). Risk assessments can cover the enterprise (a grand overview); horizontally, (systemic view of high risk clients across the organization); in a line of business, a product, a specific location, in customer profiles, and for sanctions. See Protiviti 2014b: 41-43 and 263-264.
[57] See Unger and van Waarden 2009; and Frasher 2015.
[58] Compliance employees frequently move to different companies and vendors. Teams are often "pinched" from firm to another, or to consultancies, making one wonder if any operations are truly secretive. Interviews.
[59] See 31 CFR § 1010.520 (Information Sharing Between Federal LEAs and FIs); 31 § CFR 1010.540 (Voluntary Information Sharing Among FIs); and FinCEN 314(a) Factsheet
[60] See FinCEN 2015b.
[61] French Embassy 2015: 2-3.
[62] GDPR, Recital 24c (new).
[63] Cannataci and Caruana 2014; and European Commission, 2012b.
[64] Police Data Directive COM/2012/0010, De Hert and Papakonstantinous 2012; Peers 2012; Colonna 2012; and Bignami 2007. The Framework Decision has provisions for profiling (Article 7) in police and judicial cooperation, but these will be replaced by PDD Article 9, which will put GDPR standards on LEAs. See the Profiling Project Final Report 2014: 19-20 and 26-27. While FIs must confirm the disclosure of a client's financial records in accordance with RFPA, a Protiviti FAQ advises that there are no legal processes for LEAs to gain access to SARs or supporting documentation. See Protiviti 2014b: 94.
[65] Bignami 2015. The author also addresses how governments can buy data bases from commercial data wholesalers to compose profiles of individuals. US PATRIOT § 505 expanded the use of NSLs to include US residents, visitors or US citizens who are not suspects in a criminal investigation. See Electronic Frontier Foundation, "national security letters" https://www.eff.org/issues/national-security-letters See also 31 CFR § 1010.670 (Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship).
[66] The 1992 Annunzio-Wylie Anti-Money Laundering Act and PATRIOT § 351 protect FIs from civil liability.

[67] 12 USC § 3414(a)(3) and (5)(D) restricts NSL disclosure, and Electronic Communications Privacy Act, 18 USC § 2709, Fair Credit Reporting Act, 15 USC § 1681, Right to Financial Privacy Act of 1978, 12 USC §§ 3401 *et seq.* outlines what information can be obtained from NSLs. See Doyle 2014. Levinson-Waldman (2013) finds that US authorities are allowed to keep data from 2 to 75 years. This practice raises issues for EU data protection because once the data is passed to the US government it can be kept for longer periods than EU law allows.
[68] 31 CFR § 1021.670. Weekends and holidays are included in the 120-hour time frame. See Canestri 2015. US authorities claim jurisdiction over data held abroad by US firms. Center for Democracy and Technology (2014) on the Microsoft Ireland case. § 319(a) also allows US authorities to seize foreign bank funds.
[69] See 4AMLD Article 43. The Egmont Group is an informal global association of national FIUs what promotes cooperation and standardization across AML regimes. FinCEN and EU FIUs participate MOUs in accordance with Egmont principles and transfer data via the Egmont Secure Web (ESW). The ESW is administered by FinCEN. Mitsilegas, 2003: 172. The EU shares FIU data via Fiu.net: https://www.fiu.net/; and Palboni, Kroon and Macenaite 2013. For an overview of EU FIU policies see Unger, Ferwerda, van den Broek and Deleanu 2014.
[70] Egmont Group 2013.
[71] See Korff 2015. Although responses to an AML/CTF and Privacy survey did not produce a large enough sample to utilize, two respondents indicated they have received data requests from LEAs outside their jurisdiction. The question did not ask the specific nature of the request. Question: "Has your department ever received an informal or formal request for information from law enforcement officials who were outside your office's geographical jurisdiction?"
[72] Umbrella Agreement 2015; and Judicial Redress Act of 2016.
[73] Bignami 2015 covers the data protection limitations of the Privacy Act. She says that the Presidential Policy Directive 28 (2014) attempted to address privacy for non-US persons in foreign intelligence surveillance by imposing some purpose limitations on bulk data collections (28-29).
[74] Act refers to 5 USC §552(a)
[75] See 18 USC §§ 1956 and 1957 for a list of unlawful activities.
[76] See WP29 2015; GDPR Recital 14; and Police Data Protection Directive, COM 2012/0010 2015.
[77] Client and customer are used interchangeably (despite their legal differences in US law).
[78] FinCEN 2014.
[79] 12 CFR §§ 208.63(b), 211.5(m), 211.24(j) (Federal Reserve); 12 CFR § 326.8(b) (FDIC); 12 CFR § 748.2(b) (NCUA); 12 CFR § 21.21 (OCC); and 31 CFR § 1020.220 (FinCEN). PATRIOT § 326 requires a residential or business address for individuals or a contact for next of kin or other contact. 4AMLD Article 41 is reinforced by the GDPR.
[80] See 31 CFR § 1020.100, 31 CFR § 1020.315(b) (1-4), CFR § 1020.220. PATRIOT § 326. 31 CFR § 1010.312 requires identification for currency transactions in excess of $10,000.
[81] See European Central Bank 2013, Comment 3.1; EDPS 2013, Comment 3.1.3; and WP29 2011b, Rec. 24.
[82] See European Commission 2009: 43. 4AMLD requires all customers to receive notification of the purposes for which their data is collected in Article 41(3).
[83] 4AMLD Article 13.
[84] WP29 2011a and 2011b noted access problems since confidentiality requirements do not allow authorities to divulge if an individual was the subject of a SAR investigation even if they have been exonerated. There are no rights to access FI or FIU held SARs in the US. FIs usually keep documentation of SAR investigations even when a SAR is not filed.
[85] GDPR Article 5(d).
[86] FATF 2013; 4AMLD Recital 33, Articles 20, 22, and 23. US firms are obligated to do EDD on personal banking and foreign clients via PATRIOT 312 and 31 USC § 5318, and there are special measures if a non-US person is opening a foreign bank account as defined by 31 CFR § 1010.620. See PATRIOT § 315 for foreign corruption offenses as ML crimes. For US domestic PEPs see FinCEN 2011b:38.
[87] FFIEC BSA Examination Manual: 290-291, US PATRIOT §§ 312 and 326. See FinCEN 2008.
[88] EDPS 2013, Rec. 80; and WP29 2011b Rec. 2.
[89] See BerlinRisk 2015.
[90] World-Check 2008.
[91] The Wolfsberg Group (2008) has also recommended that PEPs be removed from FI lists after 1 year out of office.
[92] See FATF 2014. BO also includes trusts, which are not covered in this analysis.
[93] 4AMLD Articles 3(6) and 3(7). Alcara 2013 provides an excellent summary. FinCEN 2014.
[94] Directive 2013/34/EU.
[95] Thanks to Dave Van Moppes for this point.
[96] Gascoigne 2014.
[97] 4AMLD Articles 13 and 14.
[98] FinCEN estimates FIs will spend "between $700 million and $1.5 billion through 2025" to collect BO information. Adams 2015a. The 2015 ACAMS/Dow Jones survey found that only 10% of respondents worked for companies that required 100% verification.
[99] See FATF 2014b; and G20 statement, Australia 2014: http://www.mofa.go.jp/files/000059869.pdf

[100] See Elgin-Cossart and Zerden 2015. The US Treasury is reconsidering BO registries in the wake of the Panama Papers leaks. See Clozel.
[101] 4AMLD Article 30(9). The GDPR allows registries in Recital 86. "Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject."
[102] For example, see GDPR Articles 44(g) and 44(2).
[103] Both 4AMLD and the BSA require FIs keep their data accessible to authorities and regulators. For foreign correspondent banking the US has a 120-hour rule. See PATRIOT § 319(b).
[104] See 4AMLD Recitals 144 and 145 and Articles 30 and 40.
[105] EDPS 2013, Recommendation 28. The GDPR addresses the topic in Article 30. See European Commission 2012; ENISA (EU Agency for Network and Information Security); International Standards Organization (ISO) 27018:2014; National Institute of Standards and Technology (NIST) 2013.
[106] GDPR Recitals 30 and 53, Articles 17 and 18(2a).
[107] GDPR Articles 31, 33 and 51.
[108]See 31 CFR § 1010.410 on types of records maintained, and 31 CFR § 1010.430 on the retention period. 31 CFR § 1020.220(a)(3)(ii); and Protiviti, 2014b: 64.
[109] Center for Democracy & Technology 2014. One interviewee suggested placing servers within legally restrictive jurisdictions to act as a 'check' on data access for employees within a firm and to protect the FI from foreign authority requests.
[110] 4AMLD Article 2 credit institutions; financial institutions; auditors, external accountants and tax advisors;
legal professionals, trust or company service providers; estate agents; persons trading in goods in cash in an amount of EUR 10 000; and gambling services.
[111] US PATRIOT § 326.
[112] See Boyd 2006: 12; Helller 2004; and FTC Safeguard Rule 2006.
[113] 4AMLD Recital 36. They are also known as Third Party Service Providers (TPSPs).
[114] 95/46/EC Recital 30 allowed Member States to determine "the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies." Article 7, "Member States shall provide that personal data may be processed only if: (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed…" See also 4AMLD Recital 35 and 36.
[115] GDPR Article 26.
[116] ACAMS/Dow Jones Survey 2015.
[117] De Busser 2014: 92.
[118] De Busser: 97-99. Under 95/46/EC anyone could be identified with varying amounts of effort so PII is includes data that identifies or *may* identify an individual. In this case, aggregated or statistical data is not applicable when individuals cannot be determined. However, researchers have noted that there is no such thing as anonymized or pseudonymized data and in certain circumstances it is possible to identify persons within these figures, sometimes referred to as "re-identification." See Ohm 2010. The GDPR addresses anonymous and pseudonymisation in Recitals 23, 23a, and 23c.
[119] GDPR Recital 23 and Article 4(1). Emphasis added.
[120] ACAMS/ Dow Jones Survey 201; Kaufman/Rossin 2015 (Florida only) and LexisNexis Risk Solutions 2015.
[121] Interviews with compliance officers, and KYC Vendors, April and May 2015.
[122] GDPR Article 14a. Notification of vendor database use does not seem to fall under the exemptions of "disproportionate effort" or when "obtaining or disclosure is expressly laid down by Union or Member State law…" Article 14(4)(b) and (c).
[123] Schwartz and Solove 2014: 3. The authors point out that if definitions of PII cannot be reconciled then it threatens the "current status quo around second-order mechanisms for allowing data transfers. These are the U.S.-EU Safe Harbor Program, Model Contractual Clauses and Binding Corporate Rules. If the EU and U.S. cannot agree on a definition of PII, the most basic unit of information privacy law, these processes must be seen as essentially instable."
[124] IAPP/EY 2015: 86. The survey did not indicate the type of vendor or vendor roles in the company. As of September 2015, the FTC's Safe Harbor site showed 200 companies registered and certified as "financial services" and all major KYC database vendors were listed and certified as "information services."
[125] GDPR Article 9(1).
[126] GDPR Article 9a. See Korff 2002 and 2010 re Member State law under 95/46/EC and sensitive data.
[127] See 18 USC §§ 1956 and 1957 for specifics. For tax reporting see Report of Foreign Bank and Financial Accounts (FBFA) and Foreign Account Tax Compliance Act (FATCA). For Federal and State laws see Doyle, 2012. Foreign

Financial Institutions sign an agreement with the US Internal Revenue Service (IRS) to "avoid a 30% withholding on US source income payments to the FFI for its own account or the accounts of its customers." (Protiviti 2014b: 576). EU interviewees stated that this was a "blatant" overextension of US regulatory reach that burdened their businesses and put them at risk for data protection violations. One US interviewee said that the EU should "do the same for foreign tax evaders in the US."

[128] 4AMLD Recital 11 and Article 3. Framework Decision 2002/475/JHA; Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances; Article 2 of the Europol Convention; Article 1(1) and Article 2(1) of the Convention on the protection of the European Communities' financial interests.

[129] See WP29 2011b, Rec. 15.

[130] See Thompson Reuters, Letter to UK Parliament Justice Committee, 2012.

[131] As suggested in EDPS 2013, Rec. 35; and WP29 2011b, Rec. 4.

[132] For example, would sharing customer data to affiliates, which is legal unless an individual opts-out in the US (Cranor, et.al. 2014), violate GDPR views on consent, or 4AMLD rules against using AML/CTF data for commercial purposes?

[133] See Egmont Group 2011 that supports this analysis. This paragraph sums responses to the author's interview question "What is the importance of enterprise data-sharing to your business and to compliance?" While respondents emphasized the legal aspects, they also cited cultural and organizational constraints to data-sharing – "It's a competitive atmosphere." Enterprise-wide data sharing should also be part of the Enterprise Risk Management (ERM) conversation within firms. It was not until recently that privacy controls were mentioned in these discussions. See Workiva, 2015.

[134] 4AMLD Article 3. This includes parent and subsidiary relationships as defined in Article 22 Directive 2013/34/EU. The GDPR addresses data protection for group undertakings in Article 4(16) and Recital 28, "A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. A central undertaking which controls the processing of personal data in undertakings affiliated to it forms together with these undertakings an entity which may be treated as "group of undertakings." Article 35 sets the requirements for DPOs within an undertaking.

[135] Concerns about bank secrecy laws and confidentially among EU firms made officers cautious about sharing SAR investigations. See European Commission 2009: 11-12.

[136] European Commission 2009.

[137] BCBS 2014.

[138] The financial services are pushing for data and recordkeeping standardization in the industry and in house, to track clients across their business. One US compliance interviewee noted their firm employed a single numerical identifier for all clients, which was aimed at maintaining pseudonymity to help solve the data protection problem across the group. They were not sure how this translated into data protection compliance.

[139] A "controlling entity" is a bank holding company, savings and loan holding company, or other company controlling 25% or more of shares of a financial institution. Agreement Corporations are state charted to use funds from national corporations to conduct international banking. Edge Corporations allow companies engaged in international business, such as trading and shipping firms, and international airlines, to provide banking services. The Federal Reserve is responsible for monitoring their activities via Regulation K 12 CFR § 211.5(k). *Farlex Financial Dictionary*, 2009.

[140] 71 Federal Regulation 13935. FFIEC BSA Examination Manual: 164-168 addresses foreign branches.

[141] See FinCEN et. al. 2006. FIs can disclose a SAR to self-regulatory organizations under certain circumstances. See 31 CFR § 1023.320.

[142] Defined in FinCEN 2010 as "…'affiliate' of a depository institution means any company under common control with, or controlled by, that depository institution. ''Under common control'' means that another company (1) directly or indirectly or acting through one or more other persons owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository institution; or (2) controls in any manner the election of a majority of the directors or trustees of the company and the depository institution. ''Controlled by'' means that the depository institution (1) directly or indirectly has the power to vote 25 percent or more of any class of the voting securities of the company; or (2) controls in any manner the election of a majority of the directors or trustees of the company. See, e.g., 12 U.S.C. § 1841(a)(2)."

[143] FinCEN 2010.

[144] See 31 CFR § 1020.320(e)(ii)(A)(2).

[145] TCH 2015: 5; and 75 FR 75593, 75595, 2010.

[146] The Clearing House LLC guidance on SAR and underlying data sharing. See TCH 2015.

[147] This is also supported by 4AMLD's third party reliance provisions as discussed in Section 3.7. KYC Exchange Net AG https://www.kyc-exchange.net/; Markit Genpact KYC http://www.kyc.com/; and SWIFT KYC Registry https://complianceservices.swift.com/kyc-registry

[148] 4AMLD Article 27.

[149] 31 CFR § 1010.540

[150] 341(b) electronic form.
[151] FinCEN 314(b) Factsheet and 2009 Factsheet. Emphasis added.
[152] Some US FIs have tried to pull their § 314(b) resources into programs like the Early Warning System, whose investors include Bank of America, JPMorgan Chase, Wells Fargo, BB&T and Capital One. Author's requests to discuss the arrangement went unanswered. See Monroe 2012.
[153] 4AMLD Article 45
[154] GDPR Recital 78 and 83.
[155] 4AMLD also requires EU and UN sanctions compliance, but is not covered in this study.
[156] PATRIOT § 352 outlines the components of an adequate US program.
[157] PATRIOT § 312 specifically applies to correspondent accounts and private banking accounts with high-risk countries. Since private banking accounts require a "minimum aggregate deposit of funds or to her assets not less than $1 million" PEPs are often involved.
[158] See Guzman 2015; 12 CFR Part § 211, and FinCEN 2015a.
[159]Douglas 2014; and O'Murchu, Arnold and Chon 2015.
[160] See Bosco, Creemers, Ferraris, Guagnin and Koops 2015; Hildebrandt 2009; Clark 199; and Profiling Project: http://profiling-project.eu
[161] Some might label this surveillance or "Dataveillance" - 'the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.' Clark 1988. For a short introduction see Böszörmenyi and Schweighofer 2015, part of the RESPECT Project http://respectproject.eu/. Protiviti 2014b: 414, notes some countries require the use of automated systems such as Switzerland, the Philippines and India.
[162] Other considerations involve the efficacy of these systems to produce actionable intelligence to state authorities. Compliance officers ask, "How much of this is useful?" Despite FATF Recommendations requiring authorities to communicate and publish statistics on the usefulness of the data they receive, officers frequently complain they have little idea of the impact their efforts serve or the Return on Investment (ROI) for intelligence.
[163] 4AMLD also uses "monitoring" referring to supervisory responsibilities. The FATF addresses monitoring in Recommendations 8 (NPOs), 10 (CDD), 12 (EDD), 13 (Correspondent Banking), 16 (Wire Transfers), 14 (Money Services), 19 (High-risk States), 20 (STRs), 22 and 23 (DNFBPs), 29 (FUIs), 23 (Cash Couriers), and 36 (International Instruments).
[164] See Protiviti 2014b: 390.
[165] WP29 2011b: 18. See also CoE 2010; and EDPS, 2013.
[166] Wolf and Viswanatha 2015 report on JPMC's backlogged investigations. Not that human judgement is full-proof from subjectivity either. Protiviti (2014b) provides a list of "red flags" for account openings that are biased against a customer's privacy concerns such as "exhibit unusual concern for secrecy" or has a "defensive stance to questions" (397). The FFIEC BSA Examination Manual, Appendix F: Money Laundering and Terrorist Financing "Red Flags," provides a long list of actions and behaviors.
[167] See The Wolfsberg Group 2009.
[168] For an overview of these and other methodologies see Protiviti, 2014a and 2014b: 409-429.
[169] See Profiling Project Final Report 2014 for citations on computer learning. Also, Booz, Allen, Hamilton 2015; Stabile 2015; and Byrne, 2016.
[170] See for example, Luca, Kleinberg and Mullainathan 2016; and Pasquale 2015.
[171] 95/46/EC Recital 15. See also CoE 1981, Article 2 (c).
[172] Austria, Bulgaria, Croatia, Estonia, Finland, Germany, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta, Romania, Slovakia, Slovenia, Sweden and the UK reported that they have transposed Article 15 into national legislation. Profiling Project Final Report 2014: 17-18.
[173] European Union Agency for Fundamental Rights 2014: 113, footnote 190.
[174] See González Fuster, De Hert and Gutwirth 2011.
[175] Profiling Project Final Report 2014: 22-27 for the development of the GDPR's profiling provisions.
[176] GDPR Article 2(1).
[177] Supported by GDPR Recital 58.
[178] Also in Article 15 (h) [Right of access for the data subject], Article 33 (2a) [Data protection impact assessment], Article 43(2e) [Transfers by way of binding corporate rules], and Article 66 (1ba) [Tasks of the European Data Protection Board].
[179] Ferraris, Bosco, and D'Angelo 2014: 14-16.
[180] Supported by GDPR Recital 59.
[181] Article 21 1(b) and (c).
[182] Article 20(1b).
[183] Recital 55 requires data portability "where the processing of personal data is carried out by automated means" and allows data subjects to "receive the personal data…which he or she has provided to a controller, in a structure, commonly used, machine-readable and interoperable format…" that can be transmitted to another controller. Data portability does

not "apply where processing of the personal data is necessary for compliance with a legal obligation…. carried out in the public interest." In this case, portability refers to data used for marketing purposes, which may get some firms into trouble who may use client data collected for AML/CTF purposes for marketing (see Section 4.10). Recital 57 and Article 18(2a).

[184] Article 21(2).

[185] Recital 75, Articles 33, 35, 36, and 37.

[186] Profiling Project Final Report 2014: 41.

[187] Council of Europe, 2008a and 2008b. None of the EU Member State DPA surveyed responded affirmatively to national implementation of Rec. 13 (2010) on profiling. See Profiling Project Final Report, 2014:19. Estonia, Finland, Germany, Lithuania and the UK reported that their regulation "meet the requirements of the Recommendation" and Italy, Slovakia, and Swiss DPAs look to it for guidance on profiling cases. The author examined 10 Member State DPA annual reports dating 2011-2014 (Austria, Belgium, Czech Republic, France, Germany, Ireland, Luxembourg, Malta, Poland, and the UK) and the EDPS 2014 Annual Report and found no complaints against banks for AML/CTF. The majority of complaints, and studies, were related to credit or debit practices.

[188] Banks are not intelligence gathering organizations, but regulatory requirements force them to invest and act as such. See Verhage, 2011 for Dutch language sources on the study of corporations as crime fighters. I will address the consequences of the securitization of banking in future Information Statecraft research.

[189] See FATF 2015; and Engen 2015.

[190] Know-Your-Customer's-Customer or KYCC, is an industry-created practice (in reaction to regulatory pressures) that assesses the risk of a customer's extended relationships, a market, or region, which has resulted from RBA demands. See Reutzel 2015.

[191] See Frasher 2015.

[192] FATF 2014a.

[193] See The World Bank 2015; Broughton 2015; and Lowery and Ramachandran 2015. Cranor et. al. 2014 shows that there is already a lot of data-sharing that might be used for these purposes. See chart on p. 11. The 2015 ACAMS/Dow Jones survey showed that 1/3 of repondents have "exited a full business line or segment" in 2014/2015 and 30% said they were planning or investigating pulling themselves for other lines in the next year.

[194] See European Commission 2009: 58-59. WP29 (2011b: 19-25) referenced this report to highlight the dangers of data sharing and profiling techniques in multinational corporations.

[195] 4AMLD includes fraud in related criminal activities in Recital 14 and Article 3. However, data protection authorities EDPS and WP29 believe that AML/CTF data should not be used in fraud detection (and vice versa) fearing "mission creep." For an overview of industry opinions on fraud see LexisNexis Risk Solutions 2015. The US considers fraud a predicate crime for ML and TF. It is to the FI's discretion to have separate fraud and AML/CTF programs, but FinCEN has supported combining them. Interviewees expressed concern as fraud and identity theft in ML and TF and felt that they should be combined internally in compliance practices and within the law.

[196] See for example de Koker and Jentzsch 2013; and Shehu 2012. Hildebrandt 2010 notes that for EU law profiling techniques makes it difficult to determine responsibility for damages incurred. See A. Scott 2015; McKendry 2014 and 2015. De Goede 2012a analyzes the avenues of charitable kinship.

[197] See De Goede 2012a.

[198] Protiviti 2015 shows that the industry is looking at these issues, but mostly from a data breach and leakage standpoint. The survey did not examine AML/CTF.

[199] For another corporate view of privacy see Bamberger and Mulligan 2015. Although not focused on AML, it presents an excellent overview of internal issues in a US-EU comparative perspective.

[200] The author attempted to conduct an anonymous online survey of AML/CTF and privacy professionals that focused on the overlap of their duties, but the response rate was too low to use in this report. Interviewees offered several explanations: the lack of industry attention to the problem; underdeveloped legal and regulatory atmosphere; and fear of regulatory backlash even for anonymous responses.

[201] ACAMS/Dow Jones did not consider data protection in its results, and the KPMG survey (p. 12) noted that privacy was *part* of a host of regulatory inconsistencies that pose difficulties in creating globally consistent AML programs (3.67 difficulty on a 5-point scale).

[202] IAPP/EY 2015: 84 and 85. AML/CTF compliance view of privacy from author's own observances and interviews.

[203] IAPP/EY 2015: 85.

[204] IAPP and Bloomberg Law 2015.

[205] Symantic 2015 and Pew Research Center 2015.

[206] IAPP /EY 2015: 13.

[207] The Privacy Bridge Group (2015) has also recommended this course for general transatlantic privacy policy.

[208] The Wolfsberg Group has been working on an AML/CTF and data privacy White Paper since 2014, but wider participation in standards setting efforts are necessary.

[209] The EU may have set the stage, but as the US has been active in some of these same efforts, although it does not use EU's language. One example can be found in FINRA's 2016 Priorities Letter which emphasized "information leakages," "data quality and governance" an examination of algorithms, back office and vendor systems, and monitoring systems.
[210] IT translates ides into code, databases, systems, and networks and are in integral part of making integrated compliance work.
[211] The IAPP/EY 2015 Report showed that privacy and finance employees do not often work together, and the majority of privacy professionals are housed within legal departments where they may not have operational knowledge. The same report noted that privacy professionals in banking are already involved in audit functions, but it did not indicate if these were in the AML/CTF arena.
[212] ACAMS and ACFCS support several academic institutions that offer this training, and the IAPP engages in similar relationships, but these need to be expanded and overlap. Thanks to Andy MacKay for his views on operations and informed intelligence cycles.
[213] The next stage of this research will involve an assessment of recommendations and actions from official bodies in the US and EU. These will be compared with industry efforts with Member State actions to determine an outline best practices that fits the three pronged approach.

7. BIBLIOGRAPHY

International Groups

Bank for International Settlements (BIS). 2015. Data-Sharing: Issues and Good Practices. http://www.bis.org/ifc/events/7ifc-tf-report-datasharing.pdf

Basel Committee on Banking Supervision (BCBS). 2014. "Sound Management of Risks Related to Money Laundering and Financing of Terrorism." http://www.bis.org/publ/bcbs275.pdf

The Egmont Group. (2013) Principles for Information Exchange Between Financial Intelligence Union. http://www.egmontgroup.org/library/download/291

-----. 2011. Enterprise-wide STR Sharing: Issues and Approaches. http://www.egmontgroup.org/library/download/116

Financial Action Task Force (FATF). 2015. Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement. https://www.coe.int/t/dghl/monitoring/moneyval/Publications/RBA-Effective-supervision-and-enforcement.pdf

-----. 2014a. Risk-Based Approach for the Banking Sector. http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html

-----. 2014b. Transparency and Beneficial Ownership" FATF Guidance. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf

-----. 2013. Politically Exposed Persons (Recommendations 12 and 22). http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

-----. 2012. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. [with 2013 and 2015 updates] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

Organization for Economic Cooperation and Development. (OECD) 1980. Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Broder Flows of Personal Data. [2013] http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Wolfsberg Group. 2009. Statement on AML Screening, Monitoring and Searching. http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Monitoring_Screening_Searching_Paper_(2009).pdf

-----. 2008. Politically Exposed Persons. http://www.wolfsberg-principles.com/pdf/faq/Wolfsberg_PEP_FAQs_(2008).pdf

World Bank. 2015. Fact-Finding Summary from De-Risking Surveys: Correspondent Banking. http://documents.worldbank.org/curated/en/2015/11/25481336/fact-finding-summary-de-risking-surveys

European Union

Council of Europe. 2012. The consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data [ETS No. 108], Modernisation of Convention 108: new proposals, DG I Rule of Law and Human Rights

-----. 2010. Recommendation CM/Rec (2010)13 The protection of individuals with regard to automatic processing of personal data in the context of profiling. http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf

-----. 2008a. Application of Convention 108 to the profiling mechanism. http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profiling_2008_en.pdf
-----. .2008b. Consultative Committee of the Convention for the protection of Individuals in regard of Automatic Processing of Personal Data, Application of Convention 108 to the Profiling mechanism, Some ideas for the future work of the Consultative Committee.
-----. 1981. Convention 108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm
-----. 1950. European Convention on Human Rights. http://www.echr.coe.int/Documents/Convention_ENG.pdf
Council Framework Decision 2002/475/JHA. EU Rules on Terrorist Offences and Related Penalties. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33168
Council Framework Decision 2008/919/JHA. Amending Framework Decision 2002/475/JHA on combating terrorism. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008F0919
Council Joint Action 98/733/JHA. Making it a criminal offence to participate in a criminal organisation in the Member States of the European Union. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31998F0733
Court of Justice of the European Union. Judgment of the Court. 2015a. ECLI:EU:C:2015:650. Case C-362/14 Maximillian Schrems v. Data Protection Commissioner. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362
-----. (2015b) ECLI:EU:C:2015:627. Opinion of Advocate General Bot. Case C-362/14 Maximillian Schrems v. Data Protection Commissioner. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450127504155&uri=CELEX:62014CC0362
Directive 2015/849/EU. The Prevention of the use of the financial system for the purposes of money laundering or terrorist financing. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849
Directive 2013/34/EU. The annual financial statements, consolidated financial statements and related reports of certain types of undertakings. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:182:0019:0076:en:PDF
Directive 95/46/EC. The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
European Central Bank. 2013. CON/2013/32 A Proposal for a Directive on the Prevention of the use of the financial system for the purpose of money laundering and terrorist financing and on a proposal for a regulation on information accompanying transfers of funds. https://www.ecb.europa.eu/ecb/legal/pdf/c_16620130612en00020005.pdf
European Commission. 2016. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. http://europa.eu/rapid/press-release_IP-16-216_es.htm
-----. Binding Corporate Rules http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm
-----. 2013a. COM(2103) 847 final. Communication from the Commission to the European Parliament and the Council on the Functioning of Safe Harbor. http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf
-----. 2013b. MEMO/13/1059 Restoring Trust in EU-US data flows- Frequently Asked Questions. http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm
-----. 2012a. EU Cloud Computing Strategy. https://ec.europa.eu/digital-agenda/en/european-cloud-initiative
-----. 2012b. SEC(2012) 75 final. Report on Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation

in criminal matters.. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0012
-----. 2009 SEC(2009) 939. Compliance with the anti-money laundering directive by cross-border banking groups at group level. Staff Working Paper. http://aei.pitt.edu/43083/
-----. 2005. Standard Contractual Clauses for the Transfer of Personal Data to Third Countries-Frequently Asked Questions. http://europa.eu/rapid/press-release_MEMO-05-3_en.htm
European Data Protection Supervisor. 2015. Opinion 3/205 "Europe's Big Opportunity: EDPS Recommendations on the EU's Options for Data Protection Reform. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_EN.pdf
-----. Addendum to Opinion 3/2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_RECITALS_EN.pdf
-----. 2014. Guidelines on Data Protection in EU Financial Services Regulation. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_EN.pdf
-----. 2013. Opinion 2013/07 Proposal for a Directive of the European Parliament and of the council on the Prevention of the use of the Financial System for the Purpose of Money laundering and Terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-04_Money_laundering_EN.pdf
European Parliament. 2015. "MEPs close deal with Council on first ever EU Rules on Cybersecurity." http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity
-----. 2014. Report. 2013/2188 (INI) The US NSA Surveillance Programme, surveillance bodies in various Member States and their impact on EU Citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-139+0+DOC+XML+V0//EN
-----. 2012. Draft report on the 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). http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf
European Union Agency for Fundamental Rights. 2014. *Handbook on European Data Protection Law*. http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
Eurostat. 2013. Money Laundering in Europe. Statistical Working Paper. http://ec.europa.eu/eurostat/en/web/products-statistical-working-papers/-/KS-TC-13-007
Information Commissioner's Office (UK). 2014. Data Controllers and Data Processors: What the difference is and what the governance implications are. https://ico.org.uk/media/1546/data-controllers-and-data-processors-dp-guidance.pdf
General Data Protection Regulation. 2015. COM 2012/0011 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. *Statewatch.org* http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
Police Data Protection Directive. 2015. COM 2012/0010 Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. *Statewatch.org* http://www.statewatch.org/news/2015/dec/eu-council-dp-dir-leas-draft-final-compromise-15174-15.pdf

French Embassy, France's Contribution. 2015. New Efforts to Combat Terrorist Financing at European Level. [Courtesy English transition] Unpublished document.

Working Party 29. 2015a. Opinion 03/2015. 3211/15/EN WP233. Draft Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences of the Execution of Criminal Penalties, and the Free Movement of Such Data. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf

-----. 2015b. Letter to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission. Re: Safe Harbour and Surveillance. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205__letter_of_the_art_29_wp_on_sh_transfers_tools_and_surveillance_.pdf

-----. 2014a. Letter to Martin Schulz, President, European Parliament. Re: BCR-P. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140612_wp29_bcr-p_general_ep_president.pdf

-----. 2014b. Letter to Viviane Reding, Vice President Commissioner for Justice, Fundamental Rights and Citizenship, European Commission. Re: Actions set out by the European Commission in order to restore trust in data flows between the EU and the US. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

-----. 2013a. Second Letter to Juan Fernando López Aguilar, Committee on Civil Liberties, Justice and Home Affairs, European Parliament. Re: Proposal for a new AML/CTF Directive. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131108_2nd_letter_aml_cft_directive_regulation_en.pdf

-----. 2013b. Advice Paper on Essential Elements of a Definition and a Provision on Profiling with the EU General Data Protection Regulation. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

-----. 2013c. WP204 00658/13/EN. Explanatory Document on the Processor Binding Corporate Rules [Revised 22 May 2015] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf

-----. (2013d) Letter to Juan Fernando López Aguilar, Committee on Civil Liberties, Justice and Home Affairs, European Parliament. Re: Proposal for a new AML/CTF Directive. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130404_aml_letter_to_ep_en.pdf

-----. (2011a) Opinion 14/2011 01008/2011/EN WP186 Data Protection Issues Related to the Prevention of Money Laundering and Terrorist Financing. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf

-----. (2011b) Annex to WP186. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en_annex.pdf

-----. (2010) 00264/10/EN WP169, Opinion 1/2010 on the concepts of controller and processor. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

United States

Anti-Money Laundering & Financial Privacy & Data-Access

1970 Bank Secrecy Act 31 USC *et. seq* and 31 CFR Chapter X
https://www.fincen.gov/statutes_regs/bsa/
1970 Fair Credit Reporting Act (FCRA) 15 USC 1681
https://www.law.cornell.edu/uscode/text/15/chapter-41/subchapter-III
1978 International Emergency Economic Powers Act (IEEPA) 50 USC 1701
https://www.law.cornell.edu/uscode/text/50/chapter-35
1978 Foreign Intelligence Surveillance Act (FISA) 50 USC Chapter 36
https://www.law.cornell.edu/uscode/text/50/chapter-36
1978 Right to Financial Privacy Act (RFPA) 12 USC 3401
https://www.law.cornell.edu/uscode/text/12/chapter-35
1986 Electronic Communications Privacy Act (ECPA)
(Amendments, 2015-16) https://www.congress.gov/bill/114th-congress/senate-bill/356
Wiretap Act, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119
Stored Communication Act, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121
Pen Register Act, https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206
1986 Money Laundering Control Act, 18 USC 1956 and 1957.
http://www.ffiec.gov/bsa_aml_infobase/documents/regulations/ml_control_1986.pdf
1988 Anti-Drug Abuse Act. https://www.gpo.gov/fdsys/pkg/FR-1995-08-02/pdf/95-18949.pdf
1992 Annunzio-Wylie Anti-Money Laundering Act https://www.gpo.gov/fdsys/granule/STATUTE-106/STATUTE-106-Pg3672/content-detail.html
1994 Money Laundering Suppression Act https://www.gpo.gov/fdsys/pkg/CREC-1994-03-21/html/CREC-1994-03-21-pt1-PgH11.htm
1998 Money Laundering and Financial Crimes Strategy Act, 31 USC 5301, 5340-5342, 5351-5355 (2012). https://www.gpo.gov/fdsys/pkg/CREC-1998-10-05/pdf/CREC-1998-10-05-pt1-PgH9480-2.pdf
1999 Financial Services Modernization Act (Gramm-Leach-Bliley, GLBA)12 USC 1811
https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/html/PLAW-106publ102.htm
2001 PATRIOT Act [US Department of Justice site with text and changes since 2001]
https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1281
2002 Sarbanes Oxley Act (SOX) 15 USC 7201 https://www.gpo.gov/fdsys/pkg/PLAW-114publ38/html/PLAW-114publ38.htm
2003 Fair and Accurate Credit Transactions Act (FACTA) 15 USC 1681
https://www.gpo.gov/fdsys/pkg/PLAW-108publ159/html/PLAW-108publ159.htm
2004 Intelligence Reform and Terrorism Prevention Act 50 USC 401
http://www.nctc.gov/docs/pl108_458.pdf
2010 Foreign Account Tax Compliance Act (FATCA) 26 USC 1471
https://www.law.cornell.edu/uscode/text/26/1471
2010 Consumer Financial Protection Act (Dodd-Frank) 12 USC 5301
https://www.law.cornell.edu/uscode/text/12/5301
Judicial Redress Act (2016) https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf
Privacy Bill of Rights Act (2015)
https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf
Umbrella Agreement. 2015. “Agreement Between the United States of America and The European Union on the Protection of Personal Information Relating to the Prevention, Investigation,

Detection, and Prosecution of Criminal Offenses." *Statewatch.org* http://statewatch.org/news/2015/sep/eu-us-umbrella-agreement-full-text.pdf

US Government

Commerce Department. Safe Harbor. http://www.export.gov/safeharbor/index.asp
Privacy Shield https://www.commerce.gov/privacyshield
Consumer Financial Protection Bureau (CFPB) "Privacy Policy for non-US persons." http://www.consumerfinance.gov/privacy/privacy-policy-for-non-us-persons/
Department of Treasury et. al. 2001. Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds of Foreign Official Corruption. http://www.federalreserve.gov/boarddocs/srletters/2001/sr0103a1.pdf
Federal Financial Institutions Examination Council (FFIEC). BSA Examination Manual http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm
Federal Trade Commission (FTC) 2012. Protecting Consumer Privacy in an Era of Rapid Change: Recommendation for Businesses and Policymakers. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
-----. Consumer Sentinel Network Data Contributors. https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors
-----. 2006. Financial Institutions and Customer Information: Complying with the Safeguards Rule. https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
-----. 2002. "The Financial Privacy Requirements of the Gramm-Leach-Bliley Act." https://www.ftc.gov/tips-advice/business-center/guidance/brief-financial-privacy-requirements-gramm-leach-bliley-act
FinCEN. 2015a. Advisory on the FATF–Identified Jurisdictions with AML/CFT Deficiencies. http://www.FinCEN.gov/statutes_regs/guidance/html/FIN-2015-A001.html
-----. 2015b. Law Enforcement Information Sharing with the Financial Industry. 2014-2015. http://www.FinCEN.gov/statutes_regs/patriot/pdf/leinfosharing.pdf
-----. 2014. Customer Due Diligence Requirements for Financial Institutions. Notice of Proposed Rulemaking. https://www.fincen.gov/statutes_regs/files/CDD-NPRM-Final.pdf
-----. 2012. Review of the Impact of FinCEN's Final Rule on the Confidentiality of Suspicious Activity Reports. https://www.fincen.gov/news_room/rp/files/SARconfidentiality_FINAL062912.pdf
-----. 2011a. Confidentiality of Suspicious Activity Reports. https://www.gpo.gov/fdsys/pkg/FR-2010-12-03/pdf/2010-29869.pdf
-----. 2011b. Foreign Corruption. The SAR Activity Review 19. https://www.fincen.gov/news_room/rp/files/sar_tti_19.pdf
-----. 2010. Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates. http://www.FinCEN.gov/statutes_regs/guidance/html/fin-2010-g006.html
-----. 2009. Guidance on the Scope of Permissible Information Sharing Covered by Section 304(b) Safe Harbor of the USA PATRIOT Act. https://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-g002.pdf
-----. 2008. Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption. https://www.fincen.gov/statutes_regs/guidance/pdf/fin-2008-g005.pdf
-----. 2007. Guidance on Suspicious Activity Report Supporting Documentation. https://www.fincen.gov/statutes_regs/guidance/html/Supporting_Documentation_Guidance.html

-----. et al. 2006. Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies. http://www.FinCEN.gov/statutes_regs/guidance/html/sarsharingguidance01122006.html
-----. 2006. Cross-Border Electronic Funds Transfer Reporting System Under the Bank Secrecy Act. https://www.fincen.gov/news_room/rp/files/CBFTFS_Complete.pdf
-----. 314(b) Factsheet. http://www.FinCEN.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf
Financial Industry Regulatory Authority (FINRA) 2016. Regulatory and Examination Priorities Letter. http://www.finra.org/sites/default/files/2016-regulatory-and-examination-priorities-letter.pdf
US Secretary of Health, Education, and Welfare. 1973. Advisory Committee on Automated Personal Data Systems. https://epic.org/privacy/hew1973report/default.html
White House. 2012. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Books, Articles & Web Sources

Accenture. 2015. North America Consumer Digital Banking Survey: Banking Shaped by the Customer. https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/Microsites/Documents17/Accenture-2015-North-America-Consumer-Banking-Survey.pdf
Adams, C. 2015a. "FinCEN Cites Costs and Benefits to Planned Customer Due Diligence Rule." *ACAMS/Moneylaundering.com*
-----. 2015b. "Sanction Civil Suits Could Expand Legal Claims of Terror Victims." *ACAMS/Moneylaundering.com*
Alacra. 2013. "Upcoming Changes to KYC Beneficial Ownership Regulatory Requirement- A Primer." https://www.alacra.com/blog/kyc-beneficial-ownership-regulations-primer/.
Allen, A. and M. Rotenberg. 2015. *Privacy Law and Society*. 3rd ed. West Academic.
De Busser, E. 2014. "Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You." *Groningen Journal of International Law* 2/2. https://groningenjil.files.wordpress.com/2015/04/grojil_vol2-issue2_de-busser.pdf
Baker and Hostetler. *US State Data Breach Charts*. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf
Balboni, P, U. Kroon and M. Macenaite. 2013. "Data Protection and Data Security by Design Applied to Financial Intelligence." In Helmut Reimer, Norbert Pohlmann and Wolfgang Schneider, eds. *ISSE 2013 Securing Electronic Business Processes*. Springer.
Bamberger, K. and D. Mulligan. 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. MIT Press.
Bennett, C. and C. Raab. 2003. *The Governance of Privacy*. Ashgate.
BerlinRisk. 2015. Political Corruption and the Assessment of Politically Exposed Persons. *LexisNexis Risk Solutions.* http://www.berlinrisk.com/Media/Downloads/BR_8_32_peps-wp-uk.pdf
Bignami, F. 2015. "The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, rights and remedies for EU citizens." http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf
-----. 2007. "Privacy and Law Enforcement in the European Union: The Data Retention Directive." *Chicago Journal of International Law* 8.

http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2304&context=faculty_scholarship

Bloustein, E. 1964. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser." *NYU Law Review* 39/962.

Böszörmenyi, J. and E. Schweighofer. 2015. "A Review of Tools to Comply with the Fourth anti-money laundering directive." *International Review of Law, Computers and Technology* 29/1.

Booz, Allen, Hamilton. 2015. Big Shifts: What's Next in AML. https://www.boozallen.com/content/dam/boozallen/documents/2015/09/machine-learning-and-data-science.pdf

Bosco, F, N. Creemers, V. Ferraris, D. Guagnin, and B.J. Koops. 2015. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities." In Gutwirth, Leenes and de Hert eds. *Reforming European Data Protection Law*. Springer.

Boyd, V. 2006. "Financial Privacy in the United States and European Union." *Berkeley Journal of International Law* 24/939.

Broughton, K. 2015. "AML Rules Create Undue 'Suspicion' of Customers, B of A Exec Says." *American Banker*. http://www.americanbanker.com/news/national-regional/aml-rules-create-undue-suspicion-of-customers-b-of-a-exec-says-1077899-1.html

Byrne, M. 2016. "Algorithms Claim to Hunt Terrorists While Protecting the Privacy of Others." *Motherboard*. http://motherboard.vice.com/read/algorithms-claim-to-hunt-terrorists-while-protecting-the-privacy-of-others

Canestri, D. 2015. "Fourth EU AML Directive: What is Missing? Section 319 PATRIOT Act and the New EU AML Directive." *European Journal of Crime, Criminal Law and Criminal Justice* 23/3.

Cannataci, J. and M. Caruana. 2014. "Report: Recommendation R (87) 15 – Twenty-five years down the line." Council of Europe. http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2013)11%20Report%20on%20data%20privacy%20in%20the%20police%20sector%20(Cannataci)%20En_(final)Rev18-02-2014.pdf

Center for Democracy & Technology. 2014. "Microsoft Ireland: Can a US Warrant Compel a US provider to Disclose Data Stored Abroad?" https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/

Centrify. 2015. "State of the Corporate Perimeter Survey Research Report: Findings from an Online Survey of 200 US IT Decision-Makers and 200 UK IT Decision-Makers." https://www.centrify.com/media/1588396/identity-survey-report.pdf

Chan, L. n.d. "Analysis of the California Financial Information Privacy Act ("SB1")" *American Banking Association*. https://www.aba.com/aba/documents/legal/SB1ABA.pdf

Clark, R. 1993. "Profiling: A Hidden Challenge to the Regulation of Data Surveillance." *Journal of Law and Information Science* 4/2.

-----. 1988. "Information Technology and Dataveillance." *Communications of the ACM* 31/5.

Clearing House LLC to FinCEN. Letter. 2015. https://www.theclearinghouse.org/~/media/files/association%20related%20documents/20150313%20cross%20border%20sar%20letter.pdf

Clozel, Lalita. 2016. "White House Pushes for New Anti-Laundering Authority." *American Banker*.

Colonna, L. 2012. "The New EU Proposal to Regulate Data Protection in the Law Enforcement Sector: Raises the Bar but not High Enough." *IRI PM 2/2012*. Stockholm University. http://www.juridicum.su.se/iri/docs/IRI-PM/2012-02.pdf

Competitive Enterprise Institute. 2000. *The Future of Financial Privacy: Private Choices versus Political Rules.* https://cei.org/studies-books/future-financial-privacy

Connolly, C. 2008. “The US Safe Harbor – Fact or Fiction?” *Galexia*. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/08_galexia_safe_harbor_/08_galexia_safe_harbor_en.pdf

Coors, C. 2010. “Headwind from Europe: The New Position of the German courts on Personality Rights after the Judgment of the European Court of Human Rights.” *German Law Journal* 11.

Cornell University Law School. Legal Information Institute (LII) https://www.law.cornell.edu/cfr/text/31/1020.320

CUPS Lab. Carnegie Mellon University. Bank Privacy. http://cups.cs.cmu.edu/bankprivacy/index.htm

Douglas, D. 2014. “France’s BNP Paribas to pay $8.9 billion to US for Sanctions Violations.” *Washingtonpost.com* http://www.washingtonpost.com/business/economy/frances-bnp-paribas-to-pay-89-billion-to-us-for-money-laundering/2014/06/30/6d99d174-fc76-11e3-b1f4-8e77c632c07b_story.html

Dow Jones and ACAMS. “2015 Global Anti-Money Laundering Survey Results.” http://images.dowjones.com/company/wp-content/uploads/sites/15/2015/03/Dow-Jones-ACAMS-AML-Survey-2015.pdf

Doyle, C. 2014. “National Security Letters in Foreign Intelligence Investigations: Legal Background.” *Congressional Research Service*. https://www.fas.org/sgp/crs/intel/RL33320.pdf

-----. 2012. “Money Laundering: An Overview of 18 USC 1956 and Related Federal Criminal Law.” *Congressional Research Service*. https://www.fas.org/sgp/crs/misc/RL33315.pdf

Durner, T. and L. Shetret. Understanding Bank De-Risking and Its Effects on Financial Inclusion. Global Center on Cooperative Security. http://www.globalcenter.org/publications/understanding-bank-de-risking-and-its-effects-on-financial-inclusion-2/

Elgin-Cossart, M. and A. Zerden. 2015. “Fighting Corruption One Goal at a Time.” *Center for American Progress*. https://cdn.americanprogress.org/wp-content/uploads/2015/09/08135300/IllicitFinancialFlows-report-FINAL.pdf

Engen, J. 2015. “Drowning in BSA Demands: How to Cope as Regulators Toughen their Stance on Bank Secrecy Act Requirements.” *American Banker*. http://www.americanbanker.com/news/consumer-finance/whats-behind-the-uptick-in-bsa-enforcement-1068937-1.html

Europe v Facebook. 2015. Prep Document. http://www.europe-v-facebook.org/Prep_CJEU.pdf

European Digital Rights. n.d. “Transfer of Data to Third Countries.” http://protectmydata.eu/topics/transfers-to-third-countries/

Farrell, H. 2002. “Negotiating Privacy across Arenas: The EU-US ‘Safe Harbor’ Discussions.” In *Common Goods: Reinventing European and International Governance*. Rowman & Littlefield.

Favarel-Garrigues, G, T. Godefroy and P. Lascoumes. 2008. “Sentinels in the Banking Industry: Private Actors and the Fight Against Money Laundering in France.” *British Journal of Criminology* 48/1.

Ferraris, V, F. Bosco, E. D’Angelo and B.J. Koops. 2014. “The Impact of Profiling on Fundamental Rights.” http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf

FitzGerald, V. 2004. “Global Financial Information, Compliance Incentives and Terrorist Funding.” *European Journal of Political Economy* 20.

Frasher, M. 2015. “Data Privacy and AML Rules on a Transatlantic Collision Course.” *American Banker*. http://www.americanbanker.com/bankthink/data-privacy-and-aml-rules-on-a-transatlantic-collision-course-1076361-1.html
-----. 2014. “The EU Privacy Ruling Won’t Hurt Innovation.” *Harvard Business Review*. https://hbr.org/2014/06/the-eu-privacy-ruling-wont-hurt-innovation/
-----. 2013a. *Transatlantic Politics and the Transformation of the International Monetary System.* Routledge.
-----. 2013b. “Adequacy Versus Equivalency: Financial Data Protection and the US-EU Divide.” *Business Horizons*. 56/6.
-----. 2012. “Updating Statecraft to the Modern Era: Finance, Information, and Regulation.” International Studies Association meeting in San Francisco, CA. Unpublished paper.
Frasher, M. and T. Selmier II. 2016. “Information Statecraft: Multinational Banks as Carriers for US & EU Law.” *Border Crossings*.
-----. 2013a. “Differing Views of Privacy Rights in the EU and US and the Resulting Challenges to International Banking: An Interview with Joseph Cannataci.” *Business Horizons*. 56/6.
-----. 2013b. “The Cross-Atlantic Tussle over Financial Data and Privacy Rights.” *Business Horizons*. 56/6.
De Goede, M. 2012a. *Speculative Security: The Politics of Pursuing Terrorist Monies.* University of Minnesota.
-----. 2012b. “The SWIFT Affair and the Global Politics of European Security.” *Journal of Common Market Studies* 50: 214-230.
Gascoigne, C. 2014. “Money Flowing Through US Banks” *Global Financial Integrity*. http://www.gfintegrity.org/press-release/gfi-urges-strengthening-of-proposed-treasury-rule-to-combat-dirty-money-at-u-s-banks/
Giraldo, J. and H. Trinkunas eds. Terrorism 2007. *Financing and State Responses: A Comparative Perspective*.
González-Fuster, G. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer.
González-Fuster, G, P. De Hert and S. Gutwirth. 2011. “Privacy and Data Protection in the EU Security Continuum.” *INEX Policy Brief* 12. https://www.ceps.eu/publications/privacy-and-data-protection-eu-security-continuum
González-Fuster, G, S. Gutwirth and E. Ellyne. 2010. “Profiling in the European Union: A High-Risk Practice.” *INEX Policy Brief* 10. https://www.prio.org/PageFiles/1522/INEX%20policy%20brief%20No%2010.pdf
Gutwirth, S, R. Leenes and P. de Hert, eds. 2015. *Reforming European Data Protection Law*. Springer.
Gutwirth, S, Y. Poullet, and P. De Hert, eds. 2010. *Data Protection in a Profiled World*. Springer.
Guzman, D. 2015. “With Lawsuit Against FinCEN and US Treasury Secretary, Macau Bank Fights its ‘Death Sentence’” *ACFCS.org* . http://www.acfcs.org/with-lawsuit-against-FinCEN-and-us-treasury-secretary-macau-bank-fights-its-death-sentence/
De Hert, P, and V. Papakonstantinous. 2012. “The Police and Criminal Justice Data Protection Directive: Comment and Analysis.” *Computers & Law Magazine of SCL* 22/6. http://www.vub.ac.be/LSTS/pub/Dehert/411.pdf
Helller, M. 2004. “In Brief: FTC: No Need to Keep Information in US” *American Banker*. http://www.americanbanker.com/issues/169_93/-221805-1.html
Hildebrandt, M. 2009. “Profiling and AML.” In Rannenberg K., Royer D., Deuker A. eds. *The Future of Identity in the Information Society*. Springer.
International Association of Privacy Professionals and EY. [IAPP-EY] Annual Privacy Governance Report 2015. https://iapp.org/resources/article/iapp-ey-annual-privacy-governance-report-2015-2/

IAPP and Bloomberg Law. 2015. Assessing and Mitigating Privacy Risk Starts at the Top. http://about.bna.com/blaw-iapp-risk-survey
De Koker, L. and N. Jentzsch. 2013. "Financial Inclusion and Financial Integrity: Aligned Incentives?" *World Development* 44.
Kaufman R. 2015. *Florida AML Compliance Survey*. http://group.kaufmanrossin.com/survey-results-2015-AML-compliance-for-banks.html
Kobrin, S. 2004. "Safe Harbors are Hard to Find: The Transatlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance." *Review of International Studies* 20.
Korff, D. 2015. "Note on the EU-US Umbrella Data Protection Agreement." Fundamental Rights European Experts Group (FREE) http://www.statewatch.org/news/2015/oct/eu-usa-umbrella-freegroup-Korff-Note.pdf
-----. 2010. "Data Protection Laws in the EU: Difficulties in meeting the challenges posed by global social and technical developments." http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf
-----. 2002. "EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws." http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE
KPMG. 2014. Global Anti-Money Laundering Survey. https://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf
Krebs, V. 2002. "Mapping Networks of Terrorist Cells." *Connections* 24/3.
Kuner, C. 2013. *Transborder Data Flow Regulation and Data Privacy Law*. Oxford.
-----. 2011. "Regulation of Transborder Data Flows under Data Protection and Privacy Law." *OECD Digital Economy Papers 187*. http://dx.doi.org/10.1787/5kg0s2fk315f-en
Lenard, T. and R. Rubin. 2012. "The FTC and Privacy: We Don't Need No Stinking Data." *American Bar Association*. http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/oct12_lenard_10_22f.authcheckdam.pdf
Lowery, C. and V. Ramachandran. 2015. "Unintended Consequences of Anti-Money Laundering Policies for Poor Countries." *Center for Global Development*. www.cgdev.org
Levinson-Waldman, R. 2013. "What the Government does with Americans' Data." *Brennen Center for Justice at New York University School of Law*. http://www.brennancenter.org/sites/default/files/publications/Data%20Retention%20-%20FINAL.pdf
LexisNexis Risk Solutions. 2015. Fraud Mitigation Study. http://www.lexisnexis.com/risk/insights/cross-industry-fraud.aspx
Luca, M, J. Kleinberg, and S. Mullainathan. 2016. "Algorithms Need Managers, Too." *Harvard Business Review* https://hbr.org/2016/01/algorithms-need-managers-too
McKendry, Ian. 2015. "The ChexSystems Probe Could Benefit the Unbanked." *American Banker* http://www.americanbanker.com/news/consumer-finance/the-chexsystems-probe-could-benefit-the-unbanked-1074005-1.html
-----. 2014. "Banks Face No-Win Scenario on AML 'De-Risking.'" *American Banker*, http://www.americanbanker.com/news/regulation-reform/banks-face-no-win-scenario-on-aml-de-risking-1071271-1.html?pg=1
Mitsilegas, V. 2003. *Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal Principles.* Klewer Law.
Moerel, L. 2011. "Back to Basics: When does EU data protection law apply?" *International Data Privacy Law* 1. http://idpl.oxfordjournals.org/content/1/2/92.full

Monroe, B. 2012. “Private Arizona Company Can Collect BSA Data with PATRIOT Act Protections: FinCEN.” *Moneylaundering.com* http://www2.acams.org/webmail/8572/220971451/0a03b3c435cb53d4488fae1aa101949a
National Conference of State Legislatures. 2015. “Privacy Protections in State Constitutions.” http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx
National Institute of Standards and Technology (NIST) 2013. “Cloud Computing Standards Roadmap.” http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf
Nissenbaum, H. 2009. *Privacy in Context*. Stanford.
Noonan, L. and J. Brunsden. 2015. “Banks warn over European Privacy Rules.” *Financial Times* http://www.ft.com/cms/s/0/3d86b628-4cca-11e5-9b5d-89a026fda5c9.htmlG
Nymity. 2015. Getting to Accountability: Maximizing Your Privacy Management Program. https://www.nymity.com/getting-to-accountability.aspx
O’Cinneide, C, M. Hunter-Henin, J. Fedtke, 2006. “German Law” in J.M. Smits ed. *Encyclopedia of Comparative Law*. Elgar.
O’Murchu, C, M. A. and G. Chon. 2015. “Standard Chartered: The Iranian Connection.” *FT.com* http://www.ft.com/cms/s/0/2b174d9c-5c81-11e5-9846-de406ccb37f2.html
Ohm, P. 2010. “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.” *UCLA Law Review* 57/1701.
Pasquale, F. 2015. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard.
Peers, S. 2012. “The Directive on data protection and law enforcement” A Missed Opportunity?” *Statewatch.org*. http://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf
Pew Research Center. 2015. “Americans’ Attitudes About Privacy, Security and Surveillance. http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf
Pillsbury and Protiviti. 2010. The Global Privacy and Information Security Landscape: Frequently Asked Questions. http://www.protiviti.com/privacyFAQ
Pinsent Masons. 2015. “More German Regulators Oppose Model Clauses for EU-US Data Transfers.” *Out-law.com* http://www.out-law.com/en/articles/2015/october/more-german-regulators-oppose-model-clauses-for-eu-us-data-transfers/
Post, R. 2001. “Three Concepts of Privacy.” *Yale Law School Faculty Scholarship Series*. http://digitalcommons.law.yale.edu/fss_papers/185
Privacy Bridges. 2015. EU and US Privacy Experts in Search of Transatlantic Privacy Solutions. https://privacybridges.mit.edu/
Prosser, W. “Privacy”. *California Law Review* 48.
Protiviti. 2015. Security and Privacy Survey. http://www.protiviti.com/en-US/Documents/Surveys/2015-IT-Security-Privacy-Survey-Protiviti.pdf
-----. 2014a. “Improve Threshold Vales Tune of Transaction Monitoring Systems by Taking a Qualitative Approach.” http://www.protiviti.com/en-US/Documents/POV/POV-AML-Threshold-Tuning-Qualitative-Approach-Protiviti.pdf
-----. 2014b. “Guide to US Anti-Money Laundering Requirements: Frequently Asked Questions.” http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-US-AML-Requirements-5thEdition-Protiviti.pdf
-----. 2013. “Views on AML Transaction Monitoring Systems.” http://www.protiviti.com/en-US/Documents/White-Papers/Industries/Views-on-AML-Transaction-Monitoring-Sytems-Protiviti-US.pdf
Regan, P. 2003. “Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows.” *Journal of Social Issues* 59/2.

Reiman, J. 1976. "Privacy, Intimacy, and Personhood." *Philosophy & Public Affairs* 6/1.
Reutzel, B. 2015. “Know Your Customer’s Customer Goes Global.” *American Banker*. http://www.americanbanker.com/news/bank-technology/know-your-customers-customer-goes-global-1074026-1.html?pg=2
Ripoll Servent, A. and A. MacKenzie. 2011. “Is the EP Still a Data Protection Champion? The Case of SWIFT.” *Perspectives on European Politics and Society* 12.
Rotenberg, M, J. Horwitz, and J. Scott. 2015. *Privacy in the Modern Age: The Search for Solutions*. The New Press.
Sammin, K. 2004. “Any Port in a Storm: The Safe Harbor, the Gramm-Leach-Bliley Act and the Problem of Privacy in Financial Services.” *George Washington International Law Review* 653/36.
Schneier, B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton.
Schriver, R. 2002. “You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission.” *Fordham Law Review* 2777/70.
Schoeman, F. 1992. *Privacy and Social Freedom*. Cambridge.
Schwartz, P. and D. Solove. 2014. “Defining Personal Data in the European Union and US. “Privacy *& Security Law Report*. http://docs.law.gwu.edu/facweb/dsolove/files/BNA-Schwartz-Solove-PII-US-EU-FINAL.pdf
Scott, A. 2015. “If Banks Can’t Solve the Derisking Dilemma, Maybe the Government Will.” *American Banker* http://www.americanbanker.com/bankthink/if-banks-cant-solve-the-derisking-dilemma-maybe-the-government-will-1073858-1.html
Scott, M. 2015. “European Court Adviser Calls Trans-Atlantic Data-Sharing Pact Insufficient.” *The New York Times*. http://nyti.ms/1OQPWDu
Shehu, A. 2012. “Promoting financial inclusion for effective anti-money laundering and counter financing of terrorism.” *Crime, Law and Social Change* 57.
Sidley Austin LLC. 2016. Essentially Equivalent: A Comparison of the Legal Order for Privacy and Data Protection in the European Union and United States. http://datamatters.sidley.com/wp-content/uploads/2016/01/Essentially-Equivalent-Final-01-25-16-9AM3.pdf
Simmel, A. 1968. “Privacy.” *International Encyclopedia of the Social Sciences* 12.
Solove, D. 2010. *Understanding Privacy*. Harvard.
Sousa de Jesus, A. 2004. “EU Data Protection in the Context of Financial Services.” *The Centre for European Policy Studies*. http://aei.pitt.edu/9429/2/9429.pdf
Spies, A. 2011. “Global Data Protection” Whose Rules Govern?” *The Sedonia Conference Journal*.
Stabile, C. 2015. “Machine Learning: Advancing AML Technology to Identify Enterprise Risk.” *ACAMS Today*. http://www.safe-banking.com/DownloadDocument.ashx?documentID=114
Strange, S. 1990. “Finance, Information and Power.” *Review of International Studies* 16.
Swire, P. 2015. “Don’t Strike Down the Safe Harbor Based on Inaccurate Views About US Intelligence Law.” *IAPP.org*. https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/
Swire, P. and K. Ahmad, 2012. “Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices. *IAPP*.
Swire, P. and R. Litan. 1998. *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive.* Brookings.
Symantec. 2015. State of Privacy Report. https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf
Tang, J. and L. Ai. 2013. "The System Integration of Anti-Money Laundering Data Reporting and Customer Relationship Management in Commercial Banks." *Journal of Money Laundering Control* 16/3.

Thompson Reuters. Letter to UK Parliament Justice Committee. 2012. “European Union Data Protection Framework Proposals.” http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/572/572vw17.htm

Turow, J, M. Hennessy, and N. Draper. 2015. “The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation.” *Annenberg School for Communication*. University of Pennsylvania. https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

TRUSTe. 2015. TRUSTe US Consumer Confidence Index. https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2015/

Unger, B, J. Ferwerda, M. van den Broek and I. Deleanu. 2014. *The Economic and Legal Effectiveness of the European Union’s Anti-Money Laundering Policy*. Edward Elgar.

Unger, B, and F. van Waarden. 2009. “How to Dodge Drowning in Data? Rule-and Risk-Based Anti-Money Laundering Policies Compared.” *Review of Law and Economics* 5/2. http://www2.econ.uu.nl/users/unger/publications/RLE3.pdf

Verhage, A. 2014. “Compliance Officers and the Uneven Playing Field in AML.” *The European Financial Review*. http://www.europeanfinancialreview.com/?p=3892

-----. 2011. *The Anti-Money Laundering Complex and the Compliance Industry*. Routledge.

Van Wasshnova, M. 2008. “Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned From the Existing System of Financial Information Exchange.” *Case Western Reserve Journal of International Law* 39.

Warren, S. and L. Brandeis. 1890. “The Right to Privacy.” *Harvard Law Review* 4. http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

Waxman, A. 2014. “Global Banks Must Make Privacy a Priority.” *American Banker*. http://www.americanbanker.com/bankthink/global-banks-must-make-privacy-a-priority-1065552-1.html

Wells Fargo. 2015. “Cyber Security and Data Privacy Survey: How Prepared Are You?” https://wfis.wellsfargo.com/insights/research/2015-Cyber-Security-and-Data-Privacy-Survey/Documents/Cyber_data_privacy_survey_white_paper_FNL.pdf

Westin, A. 1967. *Privacy and Freedom*. Athenum.

Wilmer Halle. 2008. “Ninth Circuit Partially Reinstates California Financial Privacy Law’s Affiliate Sharing Opt Out Provisions.” https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=89594

Whitman, J. 2004. “The Two Western Cultures of Privacy: Dignity versus Liberty.” *Yale Law School Faculty Scholarship Series*. http://digitalcommons.law.yale.edu/fss_papers/649

Wolf, B. and A. Viswanatha. 2015. “JPMorgan’s New Approach to Probing Suspect Transactions Sparks Internal Friction.” *Reuters.com* http://www.reuters.com/article/2015/02/12/us-jpmorgan-antimoneylaundering-insight-idUSKBN0LG0D220150212

Wolf, C. and W. Maxwell. 2015. “Why the US Is Held to a Higher Data Protection Standard Than France.” *IAPP.org*. https://iapp.org/news/a/why-the-u-s-is-held-to-a-higher-data-protection-standard-than-france/

Workiva. 2015. “From Compliance to Enterprise Risk Management.” *Compliance Week* https://www.complianceweek.com/news/roundtable-coverage/shop-talk-moving-from-compliance-to-erm

World-Check. 2008. “Refining the PEP Definition.” Edition II. http://www.world-check.com/media/d/content_whitepaper_reference/Refining_the_PEP_Definition_-_EditionII.pdf

Zarate, J. 2009. “Harnessing the Financial Furies: Smart Financial Power and National Security.” *The Washington Quarterly* http://csis.org/publication/twq-harnessing-financial-furies-smart-financial-power-and-national-security-fall-2009