Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

THOMSON REUTERS

BIG DATA

A Twenty-First Century Arms Race

BIG DATA

A Twenty-First Century Arms Race

ISBN: 978-1-61977-428-5.

June 2017

About Thomson Reuters

Thomson Reuters is the world's leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. Thomson Reuters shares are listed on the Toronto and New York Stock Exchanges (symbol: TRI). For more information, visit www.thomsonreuters.com.

About the Foresight, Strategy, and Risks Initiative

The Foresight, Strategy, and Risks Initiative (FSR) identifies trends, designs strategies, and analyzes risk to help decision makers navigate toward a more just, peaceful, and prosperous future. Using advanced tools like data analytics, scenario modeling, and simulation exercises, as well as engaging experts and the public, FSR pinpoints the most pertinent signals from the noise that become the driving force in tomorrow's reality.

CONTENTS

FOREWORD

Today's threat environment is more fast-paced and complex than ever before. Around the globe, increasingly sophisticated state and non-state actors are engaged in harming the political and economic fabric of the United States and its allies and partners. Adversaries are stepping up their use of cyber and other technologies in their attacks. Non-state actors, such as transnational organized criminals, exploit regulatory and supervisory gaps in the global financial architecture to perpetrate money laundering and fraud despite stepped up international efforts to counter them. Terrorist groups leverage cheap, easily assessable technologies to recruit adherents and plan their assaults. Needless to say, law enforcement, intelligence, and financial institutions all have their hands full trying to fend off the growing threats.

Fortunately, the big data revolution—the explosion of data and the ability to analyze them—is providing a new toolkit to help confront such a dynamic and highly unpredictable security landscape. Increasingly ubiquitous web-connected sensors and mobile technologies are creating more data, while advances in machine learning and computational power are allowing this data to be more quickly and efficiently processed. Now, US intelligence and law enforcement agencies as well as global financial institutions can connect disparate information from a variety of sources to provide wider awareness of emerging threats. And they can do it at lightning speed. Big data is not only opening the door for entirely new ways of detecting and mitigating threats, but it is also helping to streamline and accelerate existing processes.

We have seen this work firsthand at the Institute of International Finance, where we have worked to help our firms realize the benefits of the data and analytics revolution for financial institutions. While finance has long been a data-intensive industry, the big data revolution is unlocking new ways to store, access, and analyze information. Our firms are using machine learning–based algorithms to detect complex fraud, while reducing the number of false alerts. Some are using robots to autonomously act on alerts by gathering information from internal databases and systems, Internet-based sources, and social media.

To make full use of new technologies, firms and governments will need to further improve data quality and security, upgrade legacy information technology infrastructures and information sharing mechanisms, and adapt their internal cultures to fast-paced technological change. They also will need to work together to address regulatory obstacles.

In this Atlantic Council report undertaken in partnership with Thomson Reuters, five subject matter experts explore the broader security and financial implications of the big data revolution. They explain how to take advantage of the opportunities, while breaking down the challenges and policy changes that need to be addressed. Stakeholders across the security, finance, and legal communities are investing significant time and money into developing big data capabilities. The security and financial communities must stay aware of the existing analytic capabilities at their disposal and remain committed to adopting new ones to stay one step ahead of today's threats. If these tools are not properly developed and implemented, we risk becoming overwhelmed by the multitude of threats, putting the United States and the global financial system in peril.

Timothy D. Adams
President and CEO
Institute of International Finance;
Board Director
Atlantic Council

EXECUTIVE SUMMARY

We are living in a world awash in data. Accelerated interconnectivity, driven by the proliferation of Internet-connected devices, has led to an explosion of data—big data. A race is now underway to develop new technologies and implement innovative methods that can handle the volume, variety, velocity, and veracity of big data and apply it smartly to provide decisive advantage and help solve major challenges facing companies and governments.

For policy makers in government, big data and associated technologies like machine learning and artificial intelligence have the potential to drastically improve their decision-making capabilities. The national security community particularly is focused on how insight and analysis gleaned from massive and disparate datasets can help them better identify, prevent, disrupt, and mitigate threats to governments throughout the world. Big data analytics provides an unparalleled opportunity to improve the speed, accuracy, and consistency of decision making. How governments use big data may be a key factor in improved economic performance and national security.

Big data also has its drawbacks. The flood of information—some of it useful, some not—can overwhelm one's ability to quickly and efficiently process data and take appropriate action. If we fail to create and utilize methodologies and tools for effectively using big data, we may continue to drown in it. In the context of national security, lacking adequate big data tools could have profound, even deadly, consequences. However, there are steps that we can take now—steps that are already being taken in many cases—to ensure that we successfully harness the power of big data.

This publication looks at how big data can maximize the efficiency and effectiveness of government and business, while minimizing modern risks. Five authors explore big data across three cross-cutting issues: security, finance, and law.

From a security standpoint, militaries, law enforcement, and intelligence agencies have been at the forefront of developing and implementing big data capabilities. There are many opportunities for data to help improve security, from better detecting, tracking, and preventing external threats, to identifying insider threats and malicious behavior from within an organization.

The November 2015 Paris bombings renewed European law enforcement's focus on data and the important role it can play in the fight against terrorism. Before 2015, Europol's database contained 1.5 million terrorism entries; the investigation into the Paris bombings added 1.1 million entries, which highlights not only advanced collection methods, but the means to sort, filter, and analyze data to uncover leads.[1]

Police departments in the United States are also exploring the application of big data and predictive analytics to their law enforcement work. For instance, in 2015, a University of California, Los Angeles–led team of scholars and law enforcement officials used historical crime data and a mathematical model to help the Los Angeles and Kent (United Kingdom) Police Departments predict the times and places where serious crimes routinely occur in the city. The model led to lower crime rates over twenty-one months.[2] According to The Predictive Policing Company (PredPol), the success of the predictive model used by the Los Angeles Police Department and Kent Police has not only led to its permanent adoption by both departments but also sparked deployment across the United States in over fifty police departments including in Atlanta, Georgia, and Modesto, California.[3]

In the financial realm, increases in the amount and type of data that can be collected, processed, and analyzed help central banks, private banks, and other financial institutions better ensure compliance, conduct due diligence, and mitigate risk. Whether tracking cybercrime, unravelling a web of terrorist financing, or putting an end to money laundering, big data can offer these institutions new methods for ensuring economic security.

The underlying legal frameworks governing cross-border data flows are also important for helping governments use big data to increase global security. Law enforcement agencies in Europe and the United States need to be able to share threat

1 Aline Robert, "Big Data Revolutionises Europe's Fight Against Terrorism," *Euractiv,* June 23, 2016, https://www.euractiv.com/section/digital/news/big-data-revolutionises-europes-fight-against-terrorism/.

2 Stuart Wolpert, "Predictive policing substantially reduces crime in Los Angeles during months-long test," UCLA Newsroom, October 7, 2015, http://newsroom.ucla.edu/releases/predictive-policing-substantially-reduces-crime-in-los-angeles-during-months-long-test.

3 PredPol, "UCLA Study on Predictive Policing," November 11, 2015, http://www.predpol.com/ucla-predictive-policing-study/.

information to stop terrorist attacks, while banks need to be able to share due diligence information to better know their customers. Working to make legal frameworks that address data more modern, efficient, and compatible is key and just as important to global security as the algorithms designed to identify and stop potential attacks.

While big data offers many opportunities, there are still challenges that must be addressed and overcome. As new technologies and methodologies develop, we will need to work diligently to verify the trustworthiness of the collected data; properly store it and manage its utilization; reconcile divergent legal and regulatory regimes; protect individuals' privacy; and consider the ethical concerns about possible inadvertent discrimination resulting from the improper analysis and application of data.

In Chapter 1, **"Big Data: The Conflict between Protecting Privacy and Securing Nations,"** Els De Busser, a senior lecturer and senior researcher at The Hague University's Centre of Expertise Cyber Security, explains the conflicts between the data privacy and protection laws that apply to law enforcement and intelligence agencies versus those that apply to commercial entities in the private sector. The increasing localization of privacy laws has placed strain on cross-border data flows, both for law enforcement and for economic monitors. Exacerbating the problem are the different legal approaches taken in Europe and the United States, with the former tending to adopt more holistic legal frameworks, while the latter adopts more sector-specific frameworks.

In Chapter 2, **"Big Data: Exposing the Risks from Within,"** Erica J. Briscoe, a senior research scientist and lab chief scientist at the Georgia Tech Research Institute, explores how institutions can leverage big data to decrease their risk from malicious human behavior, such as insider threats. Dr. Briscoe explores how organizations can use big data techniques, including behavior modeling and anomaly detection, to identify, monitor, and prevent malicious behavior. In addition, she argues that building and maintaining trust between employers and employees is critical to discouraging malicious behavior and insider threats. To create such a trusting environment, Dr. Briscoe recommends protecting personally identifiable information to assuage fears that data could be used to negatively affect employees; monitoring both known threats and user behavior concurrently; and fostering a cybersecurity mindset, attained through a leadership-driven effort that is able to adapt to changing threats. A sidebar exploring the future of trust in an increasingly automated world is also included.

In Chapter 3, **"Big Data: The Latest Tool in Fighting Crime,"** Benjamin C. Dean, president, Iconoclast Tech, formerly a fellow for cyber-security and Internet governance at Columbia University focuses on how digital technologies and analysis of big data can be used to identify external threats, including the detection and prevention of fraud, money laundering, bribery, terrorism, and other criminal activities. There are a range of big data analytic techniques discussed, ranging from metadata collection and network analysis to data fusion and predictive analytics. A key recommendation is the need to find and invest in people who have the right knowledge, skills, and abilities to effectively and correctly use these analytic techniques. Additionally, at the strategic level, organizations need to understand how big data analytics fit into a wider organizational strategy.

In Chapter 4, **"Big Data: Tackling Illicit Financial Flows,"** Tatiana Tropina, a senior researcher at the Max Planck Institute for Foreign and International Criminal Law, explores how big data can help tackle the spread of online cybercrime and illicit financial flows—money that is illegally earned, transferred, or used. Digital technologies are facilitating illicit financial flows and the rise of an underground economy where bad actors can finance terrorism, evade taxes, and launder money. Faced with the changing nature of crime, big data promises to provide law enforcement and intelligence agencies the tools needed to detect, trace, and investigate this crime. Additionally, addressing the proper legal frameworks for cross-border criminal investigations is important. To reap the benefits of big data, governments will need to implement appropriate laws and regulations that take into account new digital technologies.

In Chapter 5, **"Big Data: Mitigating Financial Crime Risk,"** Miren B. Aparicio, counsel and senior consultant, The World Bank Global Practice, reveals how to use big data to reduce financial crime threats. This chapter analyzes best practices and new trends in anti-money laundering laws in the United States and European Union, with a focus on identifying the current gaps exploited by bad actors. Big data tools can be applied to existing risk mitigation efforts, including sanctions screening, customer profiling, and transaction monitoring, to help close existing gaps. The rise of regulation technology (regtech) solutions provides further opportunities for taking advantage of big data to mitigate financial risk. Blockchain ledger technologies and smart contracts are currently being explored by banks and financial institutions to enhance due diligence and compliance.

Samuel Klein

Program Assistant, Foresight, Strategy, and Risks Initiative, Brent Scowcroft Center on International Security, Atlantic Council

CHAPTER 1

Big Data: The Conflict Between Protecting Privacy and Securing Nations

Els De Busser

Els De Busser

Senior Lecturer, European Criminal Law; Senior Researcher, Centre of Expertise Cyber Security, The Hague University of Applied Sciences

Law enforcement and intelligence agencies need to comply with specific legal frameworks when gathering and processing personal data for the purposes of criminal investigations and national security. Private companies need to comply with specific legal frameworks when gathering and processing personal data for the purpose of commercial activities.

Both law enforcement and intelligence agencies, as well as multinational private companies, engage in cross-border data gathering. This means that two countries' legal frameworks could be applicable to their activities: one in the territory where the data are gathered and another in the territory where the data are processed—for example, personal data gathered in the European Union (EU) but processed or stored in the United States. Another conflict can arise even amongst laws in the same country—i.e., laws applicable to personal data gathered for the purpose of commercial activities versus laws applicable to personal data processed for the purpose of criminal investigations/intelligence activities.

When two or more legal frameworks contain conflicting provisions or requirements, it can create confusing situations for law enforcement or intelligence agencies and private companies. Two developments have added to the confusion. The first is the continuously increasing digitalization of the way citizens communicate, purchase items, manage finances, and do other common activities, which increase the possibility that law enforcement and intelligence authorities may need this information in the context of an investigation. The second is the growing use by private companies of cloud storage and servers located in other jurisdictions.

The last decade has shown that this dilemma is more than just theoretical. Both territorial and material conflicts have surfaced in the last several years. Fundamentally different data protection legal frameworks, combined with intensive cooperation in criminal and intelligence matters in the EU and United States, have contributed to this dilemma. In the aftermath of

the September 11, 2001, attacks on US territory, two types of data transfers were set up between the EU and the United States. First, in 2002, the US Bureau of Customs and Border Protection requested passenger name record data (PNR data) from EU air carriers flying to airports located in the United States. Then, in 2006, journalists revealed that Belgium-based private company SWIFT had transferred financial messaging data—including personal data—to the US Department of the Treasury for the purpose of investigations into the financing of terrorist activities. In both cases, agreements were ultimately signed to offer a legal framework for such transfers. In 2016, a ruling by the US Court of Appeals for the Second Circuit Court drew much attention from the industry when it ruled in favor of Microsoft in a case against the US government challenging a warrant for personal data held on a server located in Ireland.[4]

This paper focuses on these territorial conflicts, the mechanisms for preventing or solving related conflicts of laws, and the implications for relevant stakeholders.

National Laws

Criminal and national security investigations are traditionally regulated on a national level. Data protection and privacy are also typically covered in national and regional laws. Criminal law—especially criminal procedure—is traditionally regulated at the national level due to its inherent connection to the political and historical identity of a country. Hence, EU institutions have only limited competence to regulate criminal law. National security is regulated exclusively on a national level as it relates to the protection of the country and its citizens from national crises.

Data protection and privacy laws tend to be regulated on a national level as well, often in line with a regionally binding legal framework, such as the Council of Europe's (CoE) Convention 108[5] and the EU's legal instruments. Nevertheless, we can see different ways of regulating privacy and data protection. In 1999, Banisar and Davies distinguished four models: comprehensive laws, sector-specific laws, self-regulation, and technologies of privacy.[6] Whereas in Europe the first model of comprehensive or umbrella laws is clearly the preferred one, the United States uses a combination of the three other models. Apart from binding laws and rules, we should not overlook the importance of non-binding guidelines on privacy and data protection. Both the United Nations (UN) and the Organisation for Economic Co-operation and Development (OECD) have developed such rules. Of these two, the OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" is the only set of guidelines that includes a paragraph on conflict of laws.[7]

With regard to the binding legal frameworks on data protection, the aforementioned CoE Convention 108 is the widest in territorial scope as well as the most generally formulated set of standards on data protection that—in spite of the Convention currently going through a modernization—remain valid.[8]

The two most relevant[9] EU legal instruments based on the CoE standards are Directive 95/46/EC[10] covering data processing in commercial activities, and Framework Decision 2008/677/JHA[11] covering

4 On January 24, 2017, the Second Circuit Court of Appeals denied the US Department of Justice's petition for a rehearing.

5 Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention)," January 28, 1981, ETS No. 108, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

6 Daniel Banisar and Simon Davies, "Global trends in privacy protection: an international survey of privacy, data protection and surveillance laws and developments," *J. Marshall J. Computer & Info. L.*, 18 (1999): 13-14 and William J. Long and M.P. Quek, "Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise," *Journal of European Public Policy,* 9 (2002): 330.

7 OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013, http://www.oecd.org/sti/ieconomy/privacy.htm.

8 The draft protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was finalized by the responsible Ad Hoc Committee on Data Protection on June 15-16, 2016, and is awaiting adoption by the CoE Committee of Ministers following consultation of the Parliamentary Assembly. For the full text of the draft protocol, see: CoE, September 2016, "Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data," https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c.

9 These legal instruments are considered most relevant because they cover the two widest categories of data processing: processing for commercial purposes and processing for law enforcement purposes. Further legal instruments covering data protection are Regulation (EC) No 45/2001, "On The Protection Of Individuals With Regard To The Processing Of Personal Data By The Community Institutions And Bodies And On The Free Movement Of Such Data," *Official Journal of the European Communities*, L 8, January 12, 2001; Directive 2002/58/EC, "Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector," *Official Journal of the European Communities,* L 201 , July 31, 2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF.

10 Directive 95/46/EC, "On the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data," *Official Journal of the European Communities*, L 281, November 23, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.

11 Framework Decision 2008/977/JHA, "On the Protection of Personal Data Processed in the Framework of Police and

data processing for the purpose of criminal investigations and prosecutions. Both are being replaced by two newly adopted legal instruments: 1) the General Data Protection Regulation (GDPR)[12] covering data processing in commercial activities, which will be effective as of May 25, 2018; and 2) the directive on the protection of natural persons "with regard to the processing of personal data by competent authorities for the purposes" of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" and on "the free movement of such data" (directive on data protection for law enforcement purposes),[13] which will be effective as of May 6, 2018.

A significant aspect of the new GDPR is its expanded territorial application. The GDPR applies to companies that have no establishment in the EU but direct their activities at or monitor the behavior of EU citizens. This expanded scope will lengthen the list of companies from countries outside the EU—such as US companies active on the EU market—that will be confronted soon with a set of EU legal provisions with which they need to comply. One legal provision included in the GDPR that gained attention from US companies is the "right to be forgotten," which really is a right to have personal data removed when it is no longer accurate, adequate, or relevant, or if it is excessive. Thus, it is not an absolute "right to be forgotten" as the catchphrase may make one believe. The right to have inaccurate, inadequate, irrelevant, or excessive data removed has always been a right under European data protection standards, but a 2014 Court of Justice[14] ruling requiring Google to remove links containing personal data inspired a more specific "right to erasure" provision in the GDPR.[15]

The reform of the EU legal instruments on data protection also implied an expansion of the territorial scope of the directive on data protection for law enforcement purposes. The first instrument on law enforcement data protection, the 2008 Framework Decision—since expanded—covered only personal data exchanged between the member states; domestically collected data were excluded. The latter was governed only by national law. The scope of the new directive does include domestically gathered data, which means that both data transfers within the EU and data transfers outside the EU are regulated by the same directive.

"The right to have inaccurate, inadequate, irrelevant, or excessive data removed has always been a right under European data protection standards. . ."

Unlike the EU, the United States has approximately twenty sector-specific or medium-specific[16] national privacy or data security laws as well as hundreds of such laws among its states and its territories.[17] Examples of national sector-specific privacy and data protection laws include the 1996 Health Insurance Portability and Accountability Act,[18] regulating the processing and disclosure of protected health information, and the 1999 Financial Services Modernization Act,[19] also known as the Gramm-Leach-Bliley Act (GLBA), requiring financial institutions to provide their customers with a privacy notice.

With respect to criminal investigations, the US Fourth Amendment offers privacy safeguards, such as a warrant requirement, when law enforcement and intelligence authorities gather data. However, the warrant requirement, which necessitates a showing of probable cause, can slow things down. Quicker ways of obtaining data outside the scope of Fourth Amendment searches are administrative subpoenas and national security letters (NSLs). For an administrative subpoena, a warrant is not

Judicial Cooperation in Criminal Matters," *Official Journal of the European Union,* L350, December 30, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF.

12 Regulation (EU) 2016/679, GDPR, *Official Journal of the European Union*, L 119, May 4, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC.

13 Directive (EU) 2016/680, *Official Journal of the European Union,* L 119, May 4, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC.

14 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, May 13, 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

15 GDPR, Article 17.

16 Privacy or data security laws focused on a specific medium—for example an electronic medium—rather than a certain industry sector.

17 DLA Piper, "Data Protection Laws of the World, 2016, 503.

18 Health Insurance Portability And Accountability Act of 1996, Public Law (Pub.L.) 104–191, August 21, 1996, https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

19 Gramm–Leach–Bliley Act, Pub.L. 106–102, November 12, 1999, https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

Members of the European Parliament vote on the EU Passenger Name Record (PNR) Directive, which would oblige airlines to hand EU countries their passengers' data in order to help the authorities to fight terrorism and serious crimes. *Photo credit:* Reuters/Vincent Kessler.

required; rather, it is sufficient for the subpoena to be reasonable and give opportunity for the individual (hereafter, "data subject") to receive a judicial review of its reasonableness.[20] Administrative subpoenas can be used by federal agencies to order an individual to appear or deliver documents or items. The statute granting this power describes the circumstances under which subpoenas may be issued.[21]

Likewise, the 2001 USA Patriot Act[22] expanded the use of NSLs, so that any government agency investigating or analyzing international terrorism can use them.[23] Government agencies responsible for certain foreign intelligence investigations can issue NSLs to obtain customer transaction data from communication providers, banks, and credit agencies for the purpose of national security investigations.[24] The 2015 USA Freedom Act[25] strengthened judicial review of NSLs and restricted bulk collection of communications or financial records.[26] It is the use of NSLs and subpoenas in an extraterritorial manner that has caused conflicts of laws between the EU and the United States.

20 Laura K. Donahue, "Anglo-American Privacy and Surveillance," *J. Crim. L. & Criminology* 96 (2006): 1109 (footnote 278). Charles Doyle, *Administrative subpoenas in criminal investigations: a sketch*, CRS Report for Congress, March 17, 2006, https://fas.org/sgp/crs/intel/RS22407.pdf.

21 Charles Doyle, *Administrative subpoenas in criminal investigations*.

22 Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act Of 2001, Pub.L. 107–56, October 26, 2001, https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf.

23 Charles Doyle, National Security Letters in Foreign Intelligence Investigations: Legal Background, CRS Report for Congress, July 30, 2015, https://fas.org/sgp/crs/intel/RL33320.pdf.

24 Ibid.

25 USA Freedom Act, Publ.L. 114-23.

26 Charles Doyle, *National Security Letters in Foreign Intelligence Investigations*.

This brings us to the main differences facing two entities often involved in cross-border data flows and in the resulting conflict of laws between the EU and the United States. The first difference is the model of data protection legal framework that is used. The EU's reliance on omnibus legislation stands in stark contrast to the American system of sector- and data-specific laws, self-regulation, and privacy technologies. Secondly, the substance of data protection laws tends to differ between the EU and the United States. That does not mean that one offers higher data protection than the other; it means that protection is differently organized and different elements of protection are prioritized. These differences make the exchange of personal data between jurisdictions a challenge. Transferring personal data from one country to the other for the purpose of a criminal investigation or a national security investigation heightens the challenge, since such transfers should comply with two sets of data protection laws as well as two sets of criminal laws or national security laws.

Conflicts of Laws

As mentioned above, the EU and US data protection legal frameworks have led to several conflicts between the two systems. A request for EU-based personal data from US authorities would put EU companies in a dilemma. Refusing to comply with the request would trigger consequences in the United States, but complying with it may violate EU data protection laws. This section focuses on the instruments used for requesting personal data and some of the conflicts that have arisen.

Direct Access

Direct access to data is the most intrusive type of instrument for one country to obtain data held by another country, as it touches upon the sovereignty of the country granting access. Additionally, the country granting access wishes to retain some kind of control over the processing of its data by the other country. For these reasons, both countries involved will have to reach a prior agreement on the circumstances under which direct access can be allowed.

Direct access to PNR data, before those passengers board a flight from the EU to any US destination, was the subject of a number of PNR agreements between 2004 and 2012. The reason for the request for direct access was a pre-screening process that used to be conducted by US air carriers. In 2001,[27] the Aviation and Transportation Security Act moved the authority to perform a pre-screening process of passengers to the Department of Homeland Security (DHS). When the Aviation and Transportation Security Act was expanded by the 2004 Intelligence Reform and Terrorism Prevention Act,[28] an agreement with the EU became necessary due to the requirement that the European Commission (EC) assess the data protection laws of a non-EU country before a transfer of EU personal data can take place. If the EC determines that the data protection law(s) in the recipient country are not adequate, appropriate safeguards must be agreed upon. With respect to PNR data, this led to arduous negotiations between EU and US representatives resulting in several successive agreements,[29] with the most recent concluded in 2012.[30] The negotiations were complex—the main issues were the types of data included in the pre-screening, the purpose for which they would be used, and the time limits for storing the data. Another key discussion point was direct access. Giving a country *direct* access to the databases of another country's air carriers (in this case a region of twenty-eight member states) amounts to a significant sovereignty issue. When compared with a request for data or even a warrant for data, the problem was the unspecified and large amount of data.

One of the data protection standards applicable in the CoE, and thus in the EU, is the purpose limitation principle and the necessity requirement that is inherently connected to it. This means that the gathering of personal data should be done only for a specific and legitimate purpose. Processing for a purpose that is incompatible with the original purpose is not allowed unless the following conditions are met: the processing should be provided for by law, it should be necessary, and it should be proportionate. The necessity requirement includes those cases in which personal data need to be processed for the purpose of the suppression of criminal offenses. This allows, in particular, the use—by law enforcement authorities—of data that were previously gathered in a commercial setting such as data related to the purchase of an airline ticket. The necessity requirement implies, however, that the data are necessary in a specific criminal investigation, and thus mass collection of data is not considered necessary, even if such data could be useful.

27 Aviation and Transportation Security Act, Public Law no. 107-71, November 19, 2001.

28 See Section 7210, Exchange of Terrorist Information and Increased Preinspection at Foreign Airports, Intelligence Reform and Terrorism Prevention Act of 2004, Public Law no. 108-458, December 17, 2004.

29 For an overview, see Els De Busser, *EU-US Data Protection Cooperation in Criminal Matters* (Antwerp: Maklu, 2009), 358-384.

30 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (PNR Agreement), *Official Journal*, L 215, August 11, 20121, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811(01).

The purpose limitation principle is known in the United States as well. It is, however, not a general principle in the American system, but is included in specific laws only; however, while these laws may be specific, they can nonetheless have a relatively wide scope such as the 1974 Privacy Act.

For compliance with the EU data protection standard of purpose limitation, the method of accessing the data—the "push" or "pull" method—is therefore crucial. The push method means that only the data that are necessary for the purposes of a specific investigation are sent by the EU air carriers to the US Department of Homeland Security. The pull method would allow access by DHS to the air carriers' databases to retrieve the data needed. The pull method is considered the more intrusive method, taking into account that direct access to a database is granted to another country. The difference between the methods can be described as the equivalent of giving the keys to one's home to another person—the pull method—versus giving another person exactly what is necessary from one's home—the push method. The 2012 PNR agreement provides that air carriers shall be required to transfer PNR to DHS using the less intrusive push method.[31]

Subpoenas

US authorities can rely on administrative subpoenas[32] for obtaining data from private companies for the purpose of an investigation into international terrorism.[33] The conditions under which these subpoenas can be issued are laid down in statutes such as the aforementioned 1996 Health Insurance Portability and Accountability Act or the 1999 Gramm-Leach-Bliley Act (GLBA).[34] The latter protects customers' financial data including account numbers and bank balances. Financial institutions based outside the United States, but offering products or services to US customers, must also comply with the GLBA including by giving citizens a privacy notice explaining how their data would be processed.

In the aftermath of the September 11, 2001, attacks, efforts increased to investigate the financing of terrorism by setting up the Terrorist Finance Tracking Program (TFTP) of the US Treasury Department. Belgium-based SWIFT company is not a bank and does not handle money; however, it handles the financial messaging data instructing banks to transfer a specific amount of money in a specific currency from one account to another. As SWIFT organizes the majority of worldwide money transfers, it was the ideal partner for the US Treasury Department when investigating the financing of terrorism under the TFTP. The targeted data held by SWIFT included personal data. When media coverage revealed that personal data from EU citizens had been transferred from SWIFT's EU servers in the Netherlands to the US Treasury Department following what was described as "non-individualized mass requests,"[35] the European Commission and the Belgian Privacy Commission stepped in. SWIFT had been complying with US subpoenas in order to avoid prosecution in a US court, but this policy had breached Belgian data protection law. This resulted in a procedure before the Belgian Privacy Commission and in a new EU-US agreement, which provided a compromise on the safeguards for data transfers for the purposes of the Terrorist Finance Tracking Program, also known as the TFTP Agreement.[36]

Warrants

The Fourth Amendment requires probable cause for warrants issued to collect personal data for the purpose of criminal investigations, although exceptions apply.[37] Obtaining a warrant is slower in comparison to a subpoena, but offers more protection to the person involved. In the context of private companies supplying data to law enforcement, the 1986 Stored Communications Act (SCA)[38] allows the government to obtain a warrant requiring an electronic communication service provider to produce data such as customer information, emails, and other materials provided

31 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (PNR Agreement), Article 15.

32 Charles Doyle, *Administrative subpoenas in criminal investigations*.

33 See, The International Emergency Economic Powers Act (IEEPA), which followed the signing by President George W. Bush of Executive Order 13224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism," 50 USC § 1702, September 23, 2001.

34 Gramm–Leach–Bliley Act, Pub.L. 106–102, November 12, 1999.

35 Belgian Data Protection Commission, Opinion no. 37/2006, Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas, September 27, 2006.

36 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *Official Journal of the European Union*, L 195, July 27, 2010, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ%3AL%3A2010%3A195%3ATOC.

37 Applicable US legislation is 18 USC Chapter 109 and Rule 41 of the Federal Rules of Criminal Procedure.

38 Required disclosure of customer communications or records, 18 US Code (USC) § 2703, https://www.law.cornell.edu/uscode/text/18/2703.

that probable cause is shown.[39] SCA warrants are not typical warrants but have some characteristics of subpoenas and are referred to as "hybrids." The latter means that the warrant is obtained upon showing probable cause, but it "is executed like a subpoena" since "it is served on the provider and does not involve government agents entering the premises" of the provider "to search its servers and seize the e-mail account in question."[40] The matter raises questions regarding the extraterritoriality of such hybrid warrants.

That was exactly the concern in the recent Microsoft case. In 2014, when Microsoft was served with an SCA warrant for obtaining data on an email account that was located on the company's server in Ireland, the US District Court denied Microsoft's attempt to quash the warrant by stating that "even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law."[41] Microsoft appealed and received wide support from the industry in the form of several amicus curiae briefs. On July 14, 2016, the Second Circuit Court of Appeals ruled in favor of Microsoft by limiting the SCA warrants to data held within the United States regardless of whether the data pertain to a US citizen or not. It is relevant to point out here that it is unknown whether the data subject is a US citizen or not. However, the Microsoft case is not over yet; on October 13, 2016, the US government filed a petition for a rehearing,[42] and the reasons given are of essential importance for the extraterritorial seizing of data. In the appeal ruling, the Second Circuit Court acted on the assumption that providers know exactly where data are stored. The government's petition clarifies that this is not always the case[43] and stresses that due to companies working with changing facilities in different locations worldwide, "critical evidence of crimes now rests entirely outside the reach of any law enforcement anywhere in the world, and the randomness of where within an intricate web of servers the requested content resides at a particular moment determines its accessibility to law enforcement."[44]

On January 24, 2017, the appellate court denied the petition in a 4-4 vote, confirming the ruling in favor of Microsoft. Whether the case will be submitted before the Supreme Court is, at this moment, unknown. The only current alternative is a time-consuming mutual legal assistance request—but even this is not always possible due to the limited list of bilateral agreements. Scholars are expecting Congress to pass laws giving extraterritorial applicability to US warrants,[45] much like the Belgian law allowing for the extraterritorial collection of data in a criminal investigation with a *post factum* approval of the target country. Note that the CoE Cybercrime Convention allows for extraterritorial collection of data, provided that consent of the person who has the lawful authority to disclose the data is obtained.[46]

National Security Letters

Issued by high-ranking officials for the purpose of national security investigations,[47] National Security Letters are orders allowing law enforcement and intelligence agencies to obtain data by avoiding the requirements of the Fourth Amendment. Certain US laws allow for the use of NSLs[48] to order private companies such as banks, phone companies, and Internet service providers to hand over "non-content information." What can be produced in response to an NSL are log data including phone numbers or email addresses of senders and receivers, as well as information stored by banks, credit unions, and credit card companies. These disclosures may still

39 Recent cases, "In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (US District Court New York, 2014)," *Harvard Law Review*, 128 (2015): 1019.

40 In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (United States District Court, SDNY, 2014), 25.4.2014, 12, https://casetext.com/case/in-re-of-184.

41 Ibid.

42 US Court of Appeals for the Second Circuit, No. 14-2985, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation.

43 See also Orin Kerr, "The surprising implications of the Microsoft/Ireland warrant case," *Washington Post*, November 29, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/?utm_term=.b12c9264b191.

44 US Court of Appeals for the Second Circuit, No. 14-2985, In the Matter of a Warrant to Search.

45 See Jennifer Daskal, "A proposed fix to the Microsoft Ireland Case," *Just Security*, January 27, 2017, Microsoft v US, 2nd US Circuit Court of Appeals, No. 14-2985; Jennifer Daskal, "Congress needs to fix our outdated email privacy law," *Slate*, January 26, 2017, http://www.slate.com/articles/technology/ future_tense/2017/01/the_confusing_court_case_over_microsoft_data_on_servers_in_ireland.html; and Centre for Democracy and Technology, "Latest Microsoft-Ireland case ruling affirms U.S. warrants do not reach data stored outside the U.S.," January 26, 2017, https://cdt.org/press/latest-microsoft-ireland-case-ruling-affirms-u-s-warrants-do-not-reach-data-stored-outside-the-u-s/.

46 Council of Europe, Cybercrime Convention, ETS No. 185, November 23, 2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

47 50 USC §436, Requests by Authorized Investigative Agencies, and 438, Definitions.

48 The Fair Credit Reporting Act, the Electronic Communication Privacy Act and the Right to Financial Privacy Act.

include personal data that identify or enable the identification of an individual.

From an EU perspective, NSLs are problematic because they do not require probable cause; rather, the data must be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Due to the purpose limitation principle and the requirement for necessity and proportionality, the use of an NSL in the EU is highly questionable.

". . . [C]onflicts of laws create legal uncertainty and confusion for law enforcement and intelligence agencies."

In addition, the GDPR creates severe difficulties for the use of NSLs by US authorities. US companies will fall within the territorial scope of the GDPR when they offer goods or services to citizens in the EU—regardless of whether payment is required—so even free social media services such as Facebook are included. US companies will also be subject to EU jurisdiction if they monitor the behavior of EU citizens within the EU.[49] This will have a number of consequences.

First, NSLs often come with gag orders prohibiting the recipient of the NSL from disclosing their existence. The GDPR, however, introduces higher transparency standards for personal data. Thus, NSLs with a gag order requesting data on EU citizens become difficult due to these transparency rules. Article 14 of the GDPR thus creates a conflict of laws. The article lists the information that the data controller shall provide to the data subject in case personal data are processed that were not obtained directly from the data subject. The information to be provided includes the "purposes of the processing for which the data are intended [and] the legal basis for the processing; the recipients of the data" and, where applicable, that "the controller intends to transfer personal data to a [recipient in a] third country or international" organization.[50] Such transparency requirements make gag orders sent by US authorities to EU data subjects infeasible.

Second, Article 23 of the GDPR allows for restrictions to its other provisions. The duty to inform the data subject when the data were accessed for the purpose of criminal or national security investigations can also be restricted. However, such restriction is dependent on the member states or the EU creating a separate legislative measure. In order to protect the secrecy that goes with criminal and national security investigations, we can anticipate that member states will be providing for this exception in their national laws. That means that the scope of the exception, and whether or not this will include foreign law enforcement requests, is left to the member states' discretion. The relevance for private companies lies in the fines for non-compliance with Article 14 of the GDPR, which requires companies to notify the data subject. Companies that fail to comply with the GDPR risk an administrative fine of up to €20 million or up to 4 percent of the total worldwide annual turnover, whichever is higher. This means that if a US company offering electronic communications in the EU market receives an NSL with a gag order,[51] to transfer personal data to a Federal Bureau of Investigation (FBI) field office, the effect of the gag order will depend on the national law of the EU member state in which the US company has its EU headquarters. If such member state's national law provides for an exception to Article 14 for criminal investigations and national security purposes, the gag order could be upheld. If not, the company would violate the gag order if it informed the data subject to comply with Article 14, thereby facing a fine of up to €20 million or 4 percent of its total worldwide annual turnover.

Implications of Conflicts of Laws

As illustrated above, conflicts of laws create legal uncertainty and confusion for law enforcement and intelligence agencies, whose efforts in collecting cross-border information and intelligence could be blocked. If they proceed, they risk collecting information that would be inadmissible as evidence in a later criminal trial. For those countries that follow the "fruit of the poisonous tree doctrine,"[52]

49 GDPR, Article 3, §2.

50 Directive (EU) 2016/680, On The Protection Of Natural Persons With Regard To The Processing Of Personal Data By Competent Authorities For The Purposes Of The Prevention, Investigation, Detection Or Prosecution Of Criminal Offences Or The Execution Of Criminal Penalties, And On The Free Movement Of Such Data, And Repealing Council Framework Decision 2008/977/JHA, *Official Journal of the European Union*, L 119, May 4, 2016.

51 In accordance with 18 USC 2709—which was inserted by the Patriot Act—wire or electronic communications providers have a duty to comply with requests for subscriber information and toll billing records information, or electronic communication transactional records in their custody or possession. These requests can be made by the Director of the FBI as defined by 18 USC 2709. The provision concerns stored data, and not data in transit. This is relevant since the standards for obtaining stored data by the FBI are lower—NSLs do not require judicial review—than they are for data in transit—to be obtained by search warrant.

52 The fruit of the poisonous tree doctrine is a theory on the admissibility of evidence upheld by some EU member states. It means that evidence that infringes on the right to a private life is inadmissible *and* that all evidence that derived from it is also

all evidence derived from such inadmissible evidence likewise cannot be used in court. This outcome is a waste of time and resources as well as a discouragement for law enforcement and intelligence agencies.

For companies offering goods or services in several countries, conflicting laws may pose an expensive problem. In addition to regulatory fines, which are direct costs, indirect costs include legal expenses and the effect on reputation when the company is taken to court for non-compliance with—for example—a subpoena in one country because it complied with another country's law. The aforementioned Microsoft case illustrates that such proceedings can take a significant amount of time.

Citizens whose personal data are at the heart of these conflicts might have their data processed in accordance with a law that is contradictory to the law that they know. This can result in unlawful processing from their point of view. In addition, it can be problematic for such individuals to submit a complaint or initiate a proceeding in the country where the unlawful processing took place. For example, the lack of judicial redress for EU citizens under the 1974 US Privacy Act resulted in years of negotiations and ultimately led the US Congress to pass the 2016 Judicial Redress Act.[53]

Answers to Conflicts of Laws

Ad Hoc Agreements and Adequacy Requirement

Ad hoc agreements, which can resolve conflicts by presenting a hierarchy between conflicting laws and provisions, offer a possible solution. Several agreements were concluded in the past decades between EU and US authorities covering the exchange of personal data, but the EU required the United States to have an adequate level of data protection before any exchange could take place.

After the entry into force of Directive 95/46/EC, any transfer of personal data to a third country had to be preceded by an assessment of the recipient country's level of data protection. If the level of data protection was not considered adequate, the transfer would not happen unless appropriate safeguards for processing the data were in place.[54] Because the US level of data protection was not considered adequate and in order to maintain trade, a compromise was reached consisting of the self-certification system called the Safe Harbor agreement.[55] After Safe Harbor's annulment by the Court of Justice of the EU in 2015,[56] the EU-US Privacy Shield replaced it.[57]

Box 1.1. Is the adequacy requirement a form of extraterritorial application of EU legal provisions on data protection?

In essence, the adequacy requirement attaches a condition to a transfer of personal data in order to protect these data from being processed by a third state's companies or authorities in a manner that would be considered unlawful under the EU legal framework. Defining extraterritorial application of legal provisions as the interference with another state's sovereignty, we can state that the adequacy requirement to a certain extent constitutes extraterritorial application. There is an extraterritorial effect since the EU essentially imposes its level of data protection on certain third states. However, the effect is limited; if a third state does not pass the adequacy test, the transfer of data does not happen or appropriate safeguards can be agreed upon. If both parties—the EU member state transferring personal data and the recipient third state that did not pass the adequacy test—agree on such safeguards, there really is no extraterritorial application of EU legal provisions, but rather a bilateral agreement.

Ad hoc agreements can offer a solution for the conflict of laws in the context of a particular transfer of data, but they do not offer general solutions for all data transfers. Examples of ad hoc agreements are the 2012 PNR Agreement[58] and the 2010 TFTP Agreement.[59] Both these agreements, together

inadmissible. For example if during a house search, a laptop containing criminal information is seized without proper legal authority, this criminal evidence will be inadmissible if the house search was conducted illegally.

53 House Resolution (HR)1428—Judicial Redress Act of 2015, https://www.congress.gov/bill/114th-congress/house-bill/1428.

54 EU Directive, Articles 25 and 26 of Directive 95/46/EC, Data Protection Commissioner, https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapters-3-to-7-Final-Provisions/94.htm.

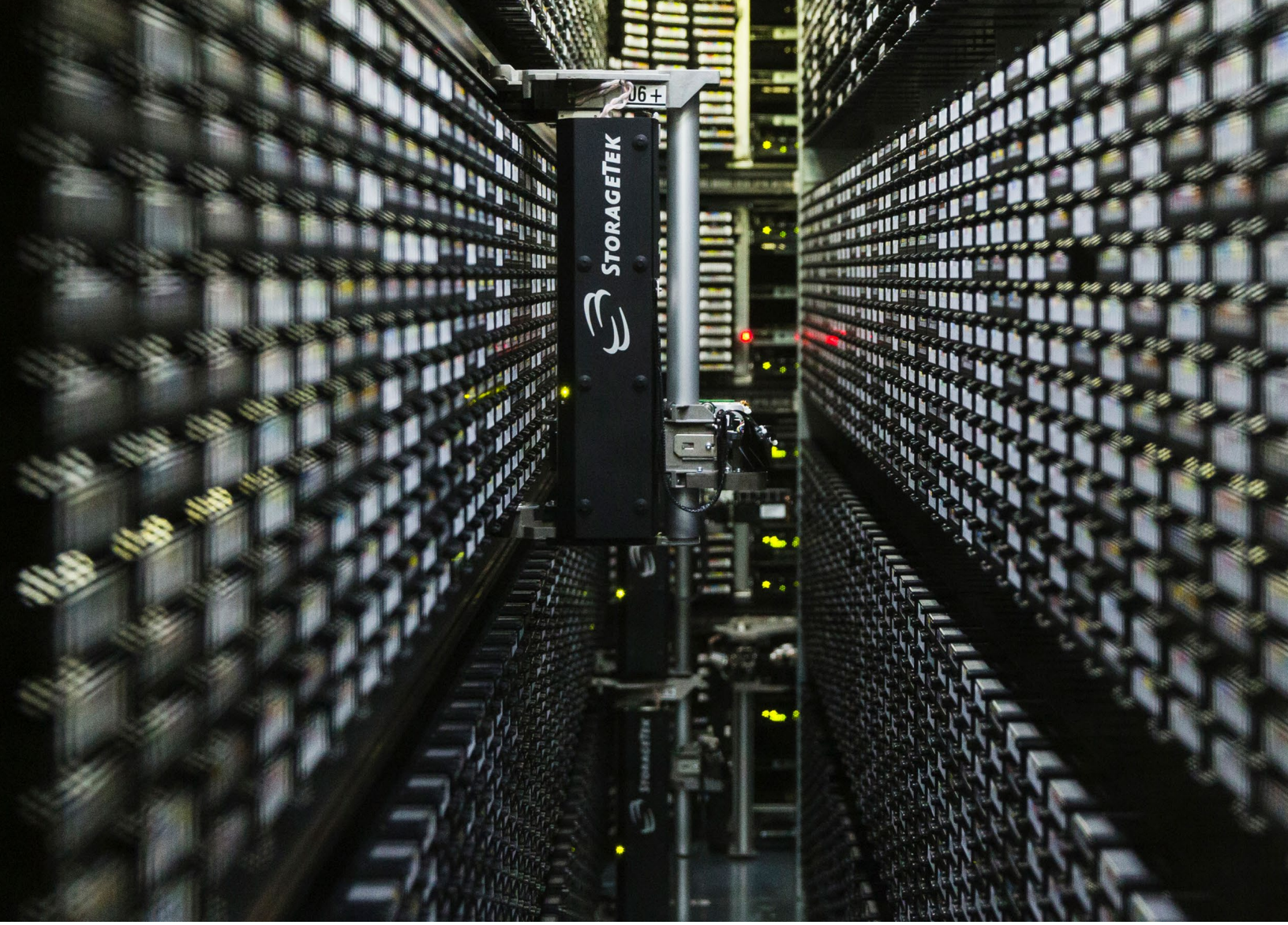
55 European Commission, Commission Decision, *Official Journal*, L 215, August 25, 2000.

56 Judgement of the Court (Grand Chamber), Schrems v Data Protection Commissioner, C-362/14, October 6, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

57 Commission Implementing Decision (EU) 2016/1250, On the Adequacy of the Protection Provided by the EU-US Privacy Shield, *Official Journal*, L 207, August 1, 2016.

58 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, *Official Journal*, L 215, August 11, 2012.

59 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *Official Journal*, L 195, July 27, 2010.



A robotic tape library used for mass storage of digital data is pictured at the Konrad-Zuse Centre for applied mathematics and computer science (ZIB), in Berlin. *Photo credit:* Reuters/Thomas Peter.

with the 2003 EU-US mutual legal assistance agreement,[60] the 2002 Europol-US Agreement,[61] and the 2006 Eurojust-US Agreement,[62] were complemented with the 2016 agreement between the United States and the EU on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses.[63] This "Umbrella Agreement" offers a "superstructure" to the prior agreements, consisting of a set of safeguards protecting data exchanged under the terms of the agreements. Most importantly, the European Commission made the signing of the Umbrella Agreement dependent on the adoption of the US Judicial Redress Act.[64] The latter expands the scope of the 1974 Privacy Act to non-US citizens, allowing them to challenge the processing of their personal data by US authorities via court redress.

Supervision by Courts and Supervisory Authorities

The aforementioned Microsoft case shows that judges, at times, rely on laws that were adopted decades ago, when a global communication infrastructure and cloud service providers were not envisioned by the legislator. Today, judges should interpret such laws and are faced with new questions on the extraterritorial obtaining of data. Supervisory authorities will also continue to play a

60 *Official Journal of the European Union,* L 181, July 19, 2003.

61 Supplemental Agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information, December 20, 2002 (not published in the *Official Journal*).

62 Agreement between Eurojust and the United States of America, November 6, 2006 (not published in the *Official Journal*).

63 Agreement on mutual legal assistance between the European Union and the United States of America, *Official Journal of the European Union*, L 336, December 10, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:336:FULL.

64 House Resolution 1428—Judicial Redress Act of 2015, February 1, 2016, https://www.congress.gov/bill/114th-congress/house-bill/1428.

role in how data transfers work in practice under the GDPR. They will continue to advise national parliaments and governments on legislative and administrative measures related to personal data processing, promote awareness of data controllers and processors of their obligations, handle complaints, and ensure consistent application and enforcement of the GDPR.

International Guidelines

The OECD guidelines described earlier are the only non-binding rules that explicitly refer to potential conflicts of data protection and privacy laws. Even though it was of essential importance that the expert group charged with developing the OECD guidelines paid attention to the issue, no detailed solution was offered. Rather, the guidelines recommend that countries work toward their own solutions. Nevertheless, the expert group mentioned a few possible solutions in the explanatory note to the guidelines.[65] Two of the solutions suggested by the expert group are highlighted here.

The expert group, first of all, stated that identifying one or more connecting factors that, at best, indicate one applicable law, is one way of approaching the issue. Connecting factors would have to be multiple and precise. Left imprecise, they would not solve the issues described earlier, for example, in the Microsoft case.[66]

A second indication offered by the expert group is to make a distinct choice for the law offering the best protection of personal data. As much as this could be a morally valuable criterion, the question is: how does one define "best protection"? When considering systems like those of the United States and the EU, where protections take different forms, the criterion of best protection could be defined only by means of general requirements including the presence of supervisory authorities, judicial complaint mechanisms, transparency, etc. Using general requirements for deciding on the most protective system defies the purpose, because both countries will fulfill the requirements—e.g., the presence of supervisory authorities—but with their own version of them.

Mutual Legal Assistance

Why do countries rely on tools involving direct access, extraterritorial subpoenas, and warrants when a request-based cooperation mechanism—based on mutual legal assistance treaties—has been in place for several decades? Mutual legal assistance in criminal matters no longer seems to be part of the narrative. Mutual legal assistance has the reputation of being slow and leaves substantial discretion to the state receiving the request in finding grounds for refusing the request.[67] In addition, mutual legal assistance requests are linked to a specific criminal investigation, leaving no chance for a bulk transfer of data.[68]

Could the solution to these difficulties lie in one expanded mutual legal assistance treaty? The idea is not that far-fetched and was even raised in the aforementioned Microsoft case,[69] but it would require significant investments in speeding up the system of mutual legal assistance requests. Investments would be needed in creating new legal provisions on allowing direct and secure communication between authorities from different countries but also in human resources to handle mutual assistance requests. One suggestion that lies along the same line of reasoning is expanding the CoE Cybercrime Convention[70] to include more types of criminal offenses.[71]

Recommendations

As described above, national rather than regional laws are the primary binding legal instruments for data protection and criminal or national security investigations.

Traditionally, ad hoc agreements have been used in an attempt to bridge conflicts of laws, but they have triggered difficult and protracted negotiations, leaving the parties and affected citizens in legal uncertainty for quite some time. Likewise, the existing mutual legal assistance mechanisms are unpopular since they do not bring quick results in a context where fast responses are essential. There are possible alternatives, however, which include the following:

65 OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 2013, "Explanatory Memorandum," http://www.oecd.org/sti/ieconomy/privacy.htm.

66 Data controlled by Microsoft as a US company but sitting on a server located in Ireland have a clear connection with both the United States (data controller) and Ireland (data location). Thus, more precise connecting factors than data control or location are necessary in order to decide on one country's law.

67 See also Jennifer Daskal, "The Un-Territoriality of Data," *Yale Law Journal*, 125 (2015): 393.

68 The latter has been at the heart of PNR data and the TFTP Agreement discussions, due to the EU's "necessity" and "proportionality" requirements.

69 Brief for Appellant, 16, In re Warrant to Search a certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV, (2d Circuit, December 8, 2014).

70 Council of Europe, Convention on Cybercrime, Articles 17-18, ETS No. 185, November 23, 2001.

71 Jennifer Daskal, The Un-Territoriality of Data, *Yale Law Journal*, 125 (2015): 394.

- Create a variation to request-based cooperation that functions in a more efficient and effective way. This would mean that responding to requests for personal data from other countries would become more automatic; however, this type of arrangement implies some form of "blind" recognition of other countries' national security and data protection regimes. The EU mutual recognition system demonstrates that such a system may fail when mutual trust among participating countries is deficient.
- Create international guidelines with a list of criteria for determining which law applies when a conflict of laws emerges. International guidelines seem feasible and attainable using the OECD guidelines as a benchmark. These guidelines should allow personal data located abroad to be obtained fast, efficiently, and most importantly, with due protection for the data subject's rights.
    - Such criteria should be established either at a supranational level—i.e., by an authority that either has the competence to legislate in a manner that legally binds the participating countries—or by means of an agreement that is ratified by countries. In the latter option, countries would commit themselves to complying with these criteria in handling extraterritorial data requests for the purpose of criminal investigations and national security investigations. An example could be taken from Article 32 of the Cybercrime Convention, but the guidance would need to be more specific with respect to consent.
    - Given the challenges of supranational fora, such as the EU, for regulating criminal and national security matters, a non-binding set of criteria may be a good option. Drawing on the adequacy decisions under Article 45 of the GDPR, the criteria should include, at a minimum, effective and enforceable data subject rights; effective administrative and judicial redress for data subjects; and one or more independent and effective supervisory authorities.[72]

Conclusion

The exponentially expanding volume of digital data creates new challenges for criminal and national security investigations. There is a tension between the need for digital data for the purpose of such investigations and the need to respect a country's sovereignty in order to protect the privacy of its citizens. Any solution to these challenges will also have to take into account the speed with which data are needed for the purpose of a criminal or national security investigation and the fact that the data might be hard to locate.

72 GDPR, Article 45.

CHAPTER 2

Big Data: Exposing the Risks from Within

Erica J. Briscoe

Erica J. Briscoe
Chief Scientist ATAS Laboratory, Georgia Tech Research Institute

A critical element in any institution is the existence of a trusting environment, which allows people to interact with one another without fear of adverse effects either on their professional or personal lives. Preservation of trust, however, is challenging. The rising number of threats to cybersecurity, fueled by an increasing reliance on data-driven devices, is coupled with a growing unease about the power that overseers tasked with ensuring that security (both corporate and government) possess as a result of their access. When taken in context with several high-profile cases of espionage, intellectual property (IP) theft, and workplace violence, both the private and public sectors are faced with a common challenge: How can institutions leverage technology to decrease their risks, especially those that involve malicious human behavior (such as insider threats)? This question cannot be answered without a careful consideration of how technology solutions affect those involved. How can these institutions minimize their vulnerability to threats, while maintaining an ethical, legal, and privacy-respecting environment? While there are no easy answers to these questions, recent research and security programs have shed some light on how a balance may be achieved, through a combination of technology and policy-driven solutions. Regardless of the responses devised to suffice today, given our increasingly automated world, institutions and the public will likely need to revisit this question continuously, ideally informed by both shared experiences and evolving research into human behavior.

Trust in Public and Private Sectors

The general concept of trust is not only complex, but its manifestation and characterization depend highly on the participating parties and the specific context in which trust exists. Whether considering individuals, governments, or machines (and all combinations thereof), there are several critical components[73] of trust. The first is that trust is made necessary

73 Christel Lane and Reinhard Bachmann, eds., *Trust within and between organizations: Conceptual issues and empirical applications* (New York: Oxford University Press, 1998).

when one party's actions are consequential or require cooperation with another. The second is that relationships require risk (e.g., that a vendor will fulfill an order on time), which trust is used to mitigate. The third is that working together requires parties to become vulnerable, where trust ensures that one party does not take advantage of the other's vulnerability. Though these aspects are usually unavoidable, trust does not mean that an organization or entity must necessarily give their partners unrestricted access to information and sensitive resources; rather, successful institutional trust usually resides in a (sometimes delicate) balance between adequate security controls and acceptable risk. This balance is not static or well-defined, but requires comprehensive approaches that allow an organization to dynamically perform identity management and access controls, as well as flexible governance coupled with education and empowerment.

Though it is widely accepted that organizations require trust, each may engender different types, either intentionally or inadvertently. Lewicki and Bunker[74] outline three types of trust that are commonly found in work environments. *Deterrence-based* trust, as it uses reprisal to deter undesired behavior, is the most explicit and fitting for new institutional relationships or for those in an environment with low levels of information control. This type is often imposed through government agency or corporate policies, where the consequences for violations are clear and able to be imposed.

Knowledge-based trust requires that the involved parties have enough familiarity to be able to predict one another's behavior. This predictability reinforces the trust over time. Interestingly, even if one party is consistently untrustworthy (e.g., an employee often fails to clock in on time though there is an explicit policy that employees must be on time), the predictability of this behavior substantiates trust (in the belief that he will always be late). This type of trust may be relevant to organizational security in many aspects. Certain violations (such as being late to work) may serve as poor indicators of a person's malicious character (or lack of trustworthiness) if that behavior is consistently inconsistent (as later discussed relevant to detecting insider threats that behave anomalously). Changes in predictability (where behavior is increasingly anomalous) is a potential red flag for diminishing trustworthiness.

The last type, *identification-based* trust, involves one party acting as an agent for the other, serving as a substitute for that entity in interpersonal transactions. Trust of this type takes time and effort to build and often results in the most surprising and devastating responses when broken. Something akin to this type of trust is found in the relationships between the federal government and its contractors, who are often seen as acting on behalf of the government; however, rather than having that bond build through time and dedication, the trust is derived from intensive security screens and usually coupled with deterrence-based methods (which are questionably reliable given the recent high-profile security breaches, for example).[75]

Building a Trusted Environment

Early in 2013, President Barack Obama issued an executive order titled "Improving Critical Infrastructure Cybersecurity"[76] describing the need for the development of a voluntary cybersecurity framework to manage cybersecurity risks associated with critical infrastructure services. This order was the federal government's acknowledgement of the extreme vulnerability of many of the country's critical systems, as well as a call for organizations to develop and instantiate processes that effectively maximize and maintain trust within and between organizations.

The president's acknowledgement of cybersecurity risks coincides with a seemingly universal interest in harnessing the power of big data, that is, the ability to derive insights from the huge amount of information generated by the many computing devices that are used every day. Though the threats to information systems take familiar forms, including common criminals, disgruntled employees, terrorists, and dishonest business partners, potential indicators of these threats may be increasingly determined by recent developments in high-performance computing, machine learning, and new analytic techniques that leverage this large-scale data collection. This utilization, in addition to the increasing sophistication of potential threats, is feeding a common realization that traditional reliance on information technology (IT) specialists alone cannot protect an enterprise from malicious behavior. Organizations must focus not only on common technological solutions (such as password change policies), but also by leveraging advances in computationally driven methods that benefit

74 Roy Lewicki and Barbara Bunker, "Developing and maintaining trust in work relationships," in Roderick Kramer and Tom Tyler, eds., *Trust in organizations: Frontiers of theory and research* (Newbury Park, CA: SAGE Publications, 1995), 114–139.

75 Ellen Nakashima, Matt Zapotosky, and John Woodrow Cox, "NSA contractor charged with stealing top secret data," *Washington Post,* October 5, 2016, https://www.washingtonpost.com/world/national-security/government-contractor-arrested-for-stealing-top-secret-data/2016/10/05/99eeb62a-8b19-11e6-875e-2c1bfe943b66_story.html.

76 White House, "Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091," February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Passengers watch a television screen broadcasting news on Edward Snowden, a contractor at the National Security Agency (NSA), on a train in Hong Kong June 14, 2013. *Photo credit:* Reuters/Bobby Yip.

from the wealth of information that is produced by modern computing systems, both at the individual and network level. Additionally, most security experts agree that a comprehensive approach that integrates best practices across policy, technology, and people while building secure, transparent relationships is a necessary and effective security strategy.

Policies and Privacy

The extent to which an employer may monitor employees is dependent on a number of factors, including the ownership of the information systems, "what the state's laws and employer's policies are, what the employee's objective expectations of privacy are," where the employee is physically located, and "whether the employer has a legitimate interest in viewing the communication."[77] Protection of employee privacy has become a popular topic, which can be broadly classified into three types: statutes restricting unauthorized access or monitoring of data; health-related information (the Genetic Information Nondiscrimination Act, the Americans with Disabilities Act, the Family and Medical Leave Act, the Health Insurance Portability and Accountability Act); and statutes protecting personally identifiable information (PII), such as identity theft statutes, the Fair and Accurate Credit Transactions Act, and state data breach laws.[78] With the blending of work and personal lives (such as on social media) and increasing efforts to improve employee home and work life balance (e.g., by allowing employees to work from home), these issues are becoming more complex and salient.[79]

77 "The Generation Gap...Tell me about it!" The Creative Network, Inc., accessed April 4, 2017, http://creativenetworkinc.com/blog/blog1.php.

78 Karen McGinnis, "The Ever Expanding Scope of Employee Privacy Protections," *ACC Charlotte Chapter Q4 2014 Newsletter,* December 2014, http://www.mvalaw.com/news-publications-373.html.

79 "The Generation Gap...Tell me about it!".

Table 2.1: Identified Insider Threat Types and Their Associated Behavior and Related Indicators.

Threat Behavior	Associated Activities	Behavioral Indicators
Espionage	Contact with foreigners Security violations Mishandling of sensitive information	Email, texting, social media Unauthorized access attempts, sharing passwords Unauthorized copying/ downloading
Fraud	Theft of financial information Modification of sensitive information	Unauthorized copying/ downloading Stress indicators, e.g., from financial hardship
Sabotage	Destruction or modification of sensitive information or software that will have detrimental results	Unauthorized access Communications exhibiting unprofessional behavior or grievances Stress indicators, such as from anger/resentment
IP Theft	Transmission of sensitive information Unjustified access to IP	Unauthorized copying/ downloading Unauthorized access attempts Foreign or competitor contacts

Expectations on the type or level of trust and privacy may be set or influenced by explicitly stated policies (at the government agency or corporate level) and laws (at the state and federal level). Often these policies run up against privacy issues, where data collected on employees meant to ensure cybersecurity, for example, may not coincide with an individual's expectations of privacy. These issues are becoming more and more relevant as the world sees an explosion of "smart" devices. The prevalence of these devices allows for a much greater ability to see into the lives and behaviors of citizens and employees. At the extreme, the situation has become a case of big brother meeting big data, where, for example, China's use of the "Sesame Credit" scoring system means that all aspects of a citizen's life may be evaluated to determine his or her trustworthiness by keeping track of individuals' financial and consumer data.[80] Additionally, formal government agency or corporate policies that require employees to sign consent to monitoring as a condition of employment may set the tone of an environment of mistrust from the beginning of an employee's tenure at an organization. This impression, along with the anxiety that arises from an employee being aware that he is under constant surveillance, may be a catalyst for subversive and malicious behavior.

Insider Threats

Perhaps the most devastating case of a breakdown in trust occurs when an individual, who is part of an organization, uses his or her access for activities that are detrimental to that organization. These insider threats are often described as current or former employees or trusted partners within an organization that abuse (or have the potential to abuse) their authorized access to the organization's system.[81] As found in a recent survey conducted by *CSO* magazine, the US Secret Service, PricewaterhouseCoopers, and the Software Engineering Institute CERT, around 30 percent of electronic attacks on both public and private organizations came from the inside.[82]

80 Celia Hatton, "China 'social credit,' Beijing sets up huge system," *BBC News*, October 2015, http://www.bbc.com/news/world-asia-china-34592186.

81 Jeffrey Hunker and Christian W. Probst, "Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2011.

82 Roger Parloff, "Spy Tech That Reads Your Mind," *Fortune*, June 30, 2016, fortune.com/insider-threats-email-scout.

Table 2.2: Example of Notable Insider Threat Cases

Insider Threat Case	Case Description	Incident Type	Threat Indicators
Xiang Dong Yu	In 2006, Yu, a product engineer for the Ford Motor Company with access to Ford trade secrets, accepted a new job at a Beijing-based automotive company that was a direct competitor of Ford. Before resigning, Yu copied 4,000 system design documents onto an external hard drive, which he later copied onto his new employer's computer.[a]	IP Theft	Email, texting, social media Unauthorized access attempts, sharing passwords Unauthorized copying/ downloading
Tim Lloyd	In 1996, after being told he was fired, Lloyd planted a software "time bomb" in a server at Omega Engineering's Bridgeport, NJ, manufacturing plant. "The software destroyed the programs that ran the company's manufacturing machines, costing Omega more than $10 million in losses."[b]	Sabotage	Unauthorized copying/ downloading Stress indicators, e.g., from financial hardship
William Sullivan	Discovered in 2007, Sullivan stole 2.3 million bank and credit card records from his employer, Certegy, a check processing company, including names, addresses, phone numbers, birth dates, and bank account information to sell.[c]	Fraud	Unauthorized access Communications exhibiting unprofessional behavior or grievances Stress indicators, such as from anger/resentment
Edward Snowden	Snowden worked as a US National Security Agency contractor who, in 2013, leaked a trove of documents about top-secret surveillance programs. He has been charged "in the United States with theft of government property, unauthorized communication of national defense information, and willful communication of classified [communications] intelligence."[d]	Espionage	Unauthorized copying, downloading

a. US Attorney's Office, Eastern District of Michigan, "Chinese national sentenced for stealing ford trade secrets," April 12, 2011, https://archives.fbi.gov/archives/detroit/press-releases/2011/de041211.htm.
b. Sharon Gaudin, "Computer sabotage verdict set aside," *Computer World*, July 12, 2000, http://www.computerworld.com/article/2596062/networking/computer-sabotage-verdict-set-aside.html.
c. Reuters, "Guilty plea in fidelity Nat'l data theft case," November 29, 2007, http://www.reuters.com/article/certegy-theft-idUSN2933291420071129.
d. Peter Finn and Sari Horwitz, "U.S. charges Snowden with espionage," *Washington Post*, June 21, 2014, https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html.

The difficulties in preventing, detecting, and countering insider threats are an increasingly major task for information security professionals, highlighted most prominently in the United States by Edward Snowden's actions involved with leaking National Security Agency data. With the collection and analysis of big data, especially through corporate insider threat programs, it is likely that the prevention and detection of malicious activities are much more feasible than previously possible; however, with this potential, there remain many questions and areas for further research.[83] Advancement in this area is also met by multiple challenges, many arising from the difficulty in balancing expectations of privacy while maintaining a trust-maximizing environment.

Types of Insider Threats and Behavior

Based on the analysis of historical cases, several descriptive taxonomies have been developed to describe insider malicious activities. For example,

83 Carly L. Huth, David W. Chadwick, William R. Claycomb, and Ilsun You, "Guest editorial: A brief overview of data leakage and insider threats," *Information Systems Frontiers 15*, 2013.

Phyo and Furnell's taxonomy[84] is based on the level(s) of information systems in which each type of incident may be detected or monitored. Internet-based activities are classified at the network level, while theft of sensitive information occurs at the operating system level. Nefarious interactions between users exist at the application level. This type of breakdown may be useful for creating a security strategy that applies to each level. Table 2.1 presents an overview of the most common types of insider threat behavior and the associated activities and indicators with each.

"The motivations behind insider threat behavior differ according to the specific individuals and their particular circumstances."

While much attention has been given to prominent insider threat cases (see table 2.2), these individuals exemplify the rarest type of threat, that which results from intentional, directed malicious behavior. These malicious insiders possess the greatest potential to cause significant harm to an organization, especially because they are likely to try to hide or cover up their behavior, making them more difficult to detect. Exploited insiders are those who may be vulnerable to the influence of outside parties, such as through social engineering (the intentional social manipulation of individuals by adversarial actors to acquire confidential or personal information) or targeted spear phishing campaigns. Careless insiders are irresponsible with regard to security, and their accidental behavior may have detrimental consequences.[85]

Motivation and Indications for Insider Threats

Careless and exploited insiders are not malicious; rather, their actions result from lack of awareness, naivety, or lax security precautions. Malicious insiders are a much more thoroughly researched group, as they pose the greatest danger to organizations and often have complicated factors contributing to their behavior. Of course, the infrequency of these events makes it difficult to develop scientific studies into the variety of motivations for such behavior; however, case studies[86] show that analyzing individual psycho-social motivations and the developmental histories of formerly trusted insiders can lead to better insight into security vulnerabilities and preventative strategies.

Based on historical cases, Shaw et al.[87] suggest six personal qualities that may contribute to malicious insider behavior:

- "False sense of entitlement" or a "lack of acknowledgement" causing a "desire for revenge"
- "Personal and social frustrations, anger, alienation, dislike of authority and an inclination for revenge"
- Computer-focused, aggressive loners, intrinsically rewarded by exploring networks, code breaking, and hacking
- "Ethical flexibility lacking moral inhibitions that would normally prevent malicious" behavior
- "Reduced loyalty identifying more with their" job or tasks than with their employer
- "Lack of empathy or inability to appreciate the impact" of behavior on others

The motivations behind insider threat behavior differ according to the specific individuals and their particular circumstances. For example, the motivation for committing fraud may be more commonly due to financial reasons,[88] while espionage may be committed for ideological or narcissistic reasons. A common pattern for insider activity is that "attacks are typically preceded by high rates of stressful events including work-related and personal events," such as following employment suspension or termination.[89] Despite known patterns, many insider activities are discovered but never made public, in order for organizations to avoid any detrimental effect on their reputational or perceived security practices.

84 William Cheswick, Steven M. Bellovin, and Aviel D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker* (Boston: Addison-Wesley Longman Publishing Co., 2003).

85 Russell Miller and Merritt Maxim, "I have to Trust someone...Don't I?," CA Technologies, 2015.

86 Stephen Band, Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak, "Comparing insider IT sabotage and espionage: A model-based analysis," (Pittsburgh, PA: Carnegie Mellon University, 2005).

87 Eric D. Shaw, Jerrold M. Post, and Kevin G. Ruby, "Inside the Mind of the Insider," *Security Management 43*, 1999.

88 Adam Cummings, Todd Lewellen, David McIntire, Andrew P. Moore, and Randall Trzeciak," Insider threat study: Illicit cyber activity involving fraud in the US financial services sector," (Pittsburgh, PA: Carnegie Mellon University, 2005).

89 Stephen Band, Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. "Comparing insider IT sabotage and espionage: A model-based analysis" No. CMU/SEI-2006-TR-026, Carnegie-Mellon University, Software Engineering Inst, 2006; Andrew P. Moore, Dawn M. Cappelli, and Randall F. Trzeciak, "The "big picture" of insider IT sabotage across US critical infrastructures," In *Insider Attack and Cyber Security*, (Santa Clara, CA: Springer-Verlag TELOS, 2008), 17-52.

Insider Threat Detection and Prevention

Security measures, such as data-loss prevention software, database activity, and network traffic monitoring programs, as well as security information event management systems, provide organizations with basic defenses, but do not much help to identify and prevent damage from insider threats. Although enterprise-wide defenses are becoming more sophisticated, the human aspect of security remains a weak link. A study of insider threat cases by the Computer Emergency Response Team (CERT) Insider Threat Center, a federally funded research and development entity at Carnegie Mellon University, found that 27 percent of insiders who became threats had drawn the attention of a co-worker because of his/her behavior prior to the incident.[90] These reports provide good support for the development of methods and systems that monitor individuals' *behavior* to detect and alert security professionals when their behavior first becomes detrimental or otherwise abnormal.

The benefit of focusing on user behavior has recently resulted in the incorporation of user behavior-focused methods as a critical component of many current enterprise systems that work to maximize cybersecurity. This often involves applications that monitor user behavior across multiple networks.[91] For example, users' computers may run an application that collects behavioral traces, which are then batched and sent to a central server to be processed at specified intervals (usually daily). The central server will also correlate and fuse information to create risk scores, which are more easily visualized and communicated to non-expert users, such as the managers who must assess the threat on a personal level.

Technical approaches for the continuous monitoring of insider behavior vary. The most straightforward method involves the direct identification of malicious activity, using what is referred to as rule-based detection, where observed events are matched against known models of threatening behavior. For example, a known threatening behavior may be the activities associated with a user accessing files that are outside of his security clearance level. While these approaches are likely to result in accurate detections, they require precise identification of the behaviors, which means that only previously *known* types of attacks will be detected.

Another clever approach that is relatively straightforward is through the use of *honeypots*. A honeypot is some type of digital asset (such as a file) that is put on a network specifically so that it can be monitored. Because the honeypot has been created to test for malicious behavior, no users should have a legitimate use for it (though it is often made to look attractive to would-be threats). This means that any interaction with the honeypot, such as a rogue user accessing it, is, by definition, suspect.

A group of much more computationally sophisticated methods use anomaly detection, which focuses on discovering rare activities within a large corpus of observation data. When considered from the perspective of an organization, the vast majority of user activities are normal and the insider threat actions are outliers.[92] Within the outlier set, insider threat activities represent an even smaller set of actions; the task is then identifying this subset of outlier actions.[93] At best, a successful insider threat detection capability would result in the identification of the actions that correspond to truly threatening behavior, but given the inherent ambiguity in determining threatening behavior, an intermediate success is the paring down of the dataset so that a human may reasonably comprehend it.[94] A successfully implemented system would allow, for example, security personnel to produce a report that would show which employees in the organization were the most anomalous or even disgruntled,[95] which may, in turn, provide an opportunity for early intervention or an increase in security measures.

Anomaly detection approaches usually require three components. First, information that represents "normal" behavior must be collected and stored. This could be employees' daily logs on activity or file accesses, for example. This information becomes the training data on which behavioral norms are modeled using a variety of machine-learning approaches, such as Markov models, support vector machines, or neural networks. Once these models of normal behavior are created (and, ideally, frequently updated), each individual's regular activity is monitored and compared against the model to determine if significant deviation occurs, which

90 Marisa Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore, Insider threat study: Illicit cyber activity in the banking and finance sector, No. CMU/SEI-2004-TR-021, Carnegie-Mellon University, Software Engineering Institute, 2005.

91 Splunk, "Machine Learning Reveals Insider Threats," last accessed March 20, 2017, https://www.splunk.com/en_us/products/premium-solutions/user-behavior-analytics/insider-threats.html.

92 David B. Skillicorn, "Computational approaches to suspicion in adversarial settings," *Information Systems Frontiers 13*, 2011.

93 Rudolph L. Mappus and Erica Briscoe, "Layered behavioral trace modeling for threat detection," International Conference on Intelligence and Security Informatics, 2013.

94 Scott Shane and David E. Sanger, "N.S.A. suspect is a hoarder. But a leaker? Investigators aren't sure," *New York Times*, October 6, 2016, http://www.nytimes.com/2016/10/07/us/politics/nsa-suspect-is-a-hoarder-but-a-leaker-investigators-arent-sure.html.

95 Roger Parloff, "Spy tech that reads your mind."

Table 2.3: Example Anomaly Detection Methods with Associated Elements

Method Elements	Method 1	Method 2
Method Type	Cross-sectional	Temporal
Entity Comparison	Individual user	Users
Baseline Population	All users / groups	Users
Baseline Feature(s)	Number of emails per day	URLs visited each day
Baseline Feature(s) Distribution	Normal (mu, sigma)	Vector of URL counts
Baseline Time Period	N/A	Last six months
Degree of Difference	Number of standard deviations from mean	Vector distance

may trigger an alert, for example, to signal a human supervisor for further investigation. Table 2.3 outlines two examples of anomaly detection methods and their distinguishing elements. Method one determines the difference in email volume between an individual user and his or her peers at one point in time compared to their average behavior over the past year. Method two compares the previous Internet activity (by creating lists of websites visited) of each user with more recent activity of that user. The primary difference between the two methods is that method one determines anomalies by comparing users to other users, while method two evaluates how a particular user changes his or her behavior over time. Comprehensive approaches that include this type of variability in methods is necessary for catching the variety of potentially malicious anomalies that may occur.

Though these detection methods usually focus on detecting deviations in normal computer usage activity, early detection methods may also concentrate on finding more subtle changes in user behavior that arise from either personal stress (which may be the motivation for becoming a threat) or the stress associated with a user knowingly committing an illegal act. The variability in a person's response to stress depends on various factors, including individual differences and the situation in which that response takes place. The effect of stress on performance can be seen as a continuum, ranging from no effect to a significant degradation in performance (e.g., the person makes errors or inadequately slow responses). This resulting change in behavior due to stress is another potential source for anomaly detection methods. Additionally, though most anomaly detection systems currently concentrate on passive detection of these types of indicators or "tells," new government research is evaluating whether these passive detectors can be combined with active indicators—those that arise from specific, intentional stimuli.[96]

While corporations are usually limited to user data collected while their employees are on corporate-owned devices, recent government employee insider threat incidents have emphasized the need to incorporate external data sources as well. This need is exacerbated by the potential detrimental effects that these employees can have with their access to highly classified information. While these workers are required to undergo fairly intensive background checks of both their financial and private lives, notable recent cases, such as that of Aaron Alexis, a former Navy reservist and military contractor who killed twelve people at the Washington Navy Yard in 2013, highlight the potential inadequacy of traditional background checks and lack of agency coordination. Former Director of National Intelligence James Clapper told Congress that what is needed is a "system of continuous evaluation where when someone is in the system and they are cleared initially, then we have a way of monitoring their behavior, both their electronic behavior on the job as well as off the job."[97] This type of employee monitoring systems might access multiple data sources in an attempt to discover patterns of suspicious behavior not caught by traditional background checks, which may be appropriate given the potential vulnerabilities for national security but seem much too invasive for ordinary citizens and employees. Examples of external sources include "private credit agencies, law enforcement databases and threat lists, military and other government records, licenses, data services

96 GCN Staff, "IARPA preps insider threat monitoring projects," *GCN*, March 19, 2015, https://gcn.com/articles/2015/03/19/iarpa-scite-insider-threat.aspx.

97 Stephen Braun, "U.S. intelligence officials to monitor federal employees with security clearances," *PBS News Hour*, March 10, 2014, http://www.pbs.org/newshour/rundown/us-intelligence-officials-monitor-federal-employees-security-clearances/.

and public record repositories,"[98] and social media, in addition to potential electronic surveillance.

Challenges

Regardless of the type or number of sources used, there are several challenges to using analytic methods to detect insider threats.[99] Of course, most malicious insiders do not wish to be detected; therefore, they try to hide their detrimental actions by concealing them within legitimate activity. This concealment makes detection much more difficult even for advanced anomaly detectors. Most algorithmic approaches also require training data, which consist of labeled cases of both known "normal" and nefarious behavior; however, the collection of these sets is difficult due to the rarity of cases and the reluctance of government agencies and companies to share information regarding their identified vulnerabilities. In application, the ratio of "bad" to "good" users in an organization is extremely low, which makes for few opportunities to test the effectiveness of implemented approaches. Given a large number of employees and multiple data sources, reducing a mass amount of information down to simplistic measures, such as risk scores, may still result in too much information for a person to process, making continuous monitoring ineffective.

Preventative Measures

While insider threat detection programs are growing more sophisticated, so should approaches that concentrate on the individual *before* he or she starts down the criminal path. These techniques probably best address the *careless* and *exploited* threat types, but may also deter *malicious* insiders by increasing the visibility of an organization's security presence. Increasingly, effort is invested in the development of security awareness and risk communication programs to raise computer users' awareness about practicing safe habits and recognizing security threats. Communications usually take five forms: warning dialogues, notices, status indicators, training, and corporate policies. These programs may also be informed by massive data analytics, usually through large-scale testing and analysis that helps to pinpoint who the most vulnerable users are.

Because malicious attacks can take many forms, so must preventative training. A growing body of research shows that there are several useful factors to a successful security awareness campaign. As one example, studies show that highly self-referencing messaging, such as those using wording that focuses on the specific individual or their personal data, is more effective than appealing to the community or corporation. A message "Protect your personal data by changing your password every month" is likely to be more effective than "IT policy requires a password change to increase cybersecurity." Also, research demonstrates that perceived threat severity can have a negative impact on self-efficacy, which is the belief that one is capable of taking effective actions to avoid the threat. These findings suggest that security messages should include references to the user and information to increase self-efficacy beliefs.

". . . Insider threat detection programs are growing more sophisticated. . ."

Evaluation of the effectiveness of security awareness campaigns often take the form of mimicked attacks initiated by security management. Subsequent security awareness messages after these "tests" are likely to be particularly effective, as users are immediately made aware of their risky behavior. With precise test construction, it is possible to ascertain exactly what attack methods are likely to result in security breaches.[100] This information, along with observed user responses, can then be used to target future messaging, campaigns, and/or training. This is more nuanced than merely understanding what types of threats people are more likely to succumb to, but which characteristics of those threats influence the users' perceptions and actions. For example, "normal" security indicators, such as a padlock icon, often go unnoticed and, therefore, serve little purpose.

Looking to the Future: Trust in an Increasingly Automated World

Traditional sources of institutional trust are usually found in the relationships that exist between employers and employees or citizens and their government, but as humans become more technology-reliant, socio-technical trust, which results from the complicated interactions between people and technology,[101] is a significant aspect in everyday life. Given the recent advances of and attention to autonomous systems, the topic

98 Stephen Braun, "U.S. intelligence officials to monitor federal employees with security clearances."

99 Amos Azaria, Ariella Richardson, Sarit Kraus, and V. S. Subrahmanian, "Behavioral analysis of insider threat: a survey and bootstrapped prediction in imbalanced data," *IEEE Transactions on Computational Social Systems* 1, No. 2, 2014.

100 Ronald C. Dodge, Curtis Carver, and Aaron J. Ferguson, "Phishing for user security awareness," *Computers & Security 26*, February 2007.

101 Albert Bandura, "Social cognitive theory: An agentic perspective," *Annual review of psychology 52*, 2001.

US Department of Homeland Security employees work in front of US threat level displays inside the National Cybersecurity and Communications Integration Center. *Photo credit:* Reuters/Kevin Lamarque.

of human-machine trust has risen to prominence in recent years[102] and will continue to increase as automation becomes more ubiquitous, requires less human involvement, and is increasingly relied upon throughout society.

Although there is an abundance of research that suggests that trust is the appropriate concept for describing human-machine interaction, there are several notable differences between that and what is understood about human-to-human trust. The most notable is that machines (even with their increasing personalization, e.g., Amazon's Echo) lack intentionality, which is a necessary component for other trust-inducing characteristics, such as loyalty, benevolence, and value congruence.[103] The asymmetry between humans and machines negates typical social cues and expectations, which in turn causes people to trust and react to machines in a dissimilar manner than they do to other humans. The facilitation of trust between humans and machines is currently most focused on the appropriate design of interfaces; however, with the increasing complexity of artificial intelligence, interface design alone is still insufficient to establish the trust that is necessary for humans to put their faith in automation. This is leading to research into how to open up the "black box," where transparency in the computational reasoning behind a machine's behavior is expected to increase the human's trust in it.[104] This transparency may be difficult in many cases, especially when the machine's reasoning mechanisms utilize representations that are not

102 Lee Hutchinson, "Four hundred miles with Tesla's autopilot forced me to trust the machine," May 22, 2016, http://arstechnica.com/cars/2016/05/four-hundred-miles-with-teslas-autopilot-forced-me-to-trust-the-machine/.

103 John Lee and Katrina A. See, "Trust in automation: Designing for appropriate reliance," *Human Factors: The Journal of the Human Factors and Ergonomics Society 46,* 2004.

104 Davide Castelvecchi, "Can we open the blackbox of AI?," Nature *538*, 2016.

human interpretable (such as deep learning networks).[105]

As fallible and risky as human behavior is, it is certainly not a given that machines are (or will be) much better. Their risks are similar to those assumed with humans, in that detrimental behavior may arise from both intentional and unintentional actions (where software bugs or hacks may cause a machine to behave unpredictably or maliciously). As technology improves, machines will become "smarter" and more social, able to communicate among themselves (creating the so-called Internet of Things),[106] and therefore less likely to require "humans in the loop." These decentralized systems, those that are not monitored by a single executive function and that have no prior knowledge of one another (but are flexible and scalable), are potentially ripe for malicious behavior. Recent approaches for managing the inherent risk within these types of systems have been inspired by other human-based techniques, such as the use of reputation.[107]

Research has found that while consumers are aware that their data are being collected on a continuous basis, they do not necessarily understand the specifics or motivations behind that collection. This lack of understanding is a source of anxiety.[108] Studies on consumer-based data have found that transparency about the use and protection of consumers' data reinforces trust, but that this trust varies across the identities of the collectors.[109] Internet-based finance firms, such as PayPal, are generally perceived to be the most highly trusted, followed by e-commerce companies, consumer electronics makers, banks and insurance companies, telecommunications carriers, large Internet companies (e.g., Google), and the government. Interestingly, retailers and entertainment-focused companies were the lowest trusted organizations, rated above only social networking sites, such as Facebook. These findings point to the fact that both government and private institutions should aspire to increase their levels of transparency in order to counteract feelings of mistrust and anxiety that may accompany necessary cybersecurity programs.

Recommendations

The following actions are recommended to create a secure yet trust-respecting environment.

- Efforts and policies toward protecting personally identifiable information may assuage some of the fears that collected information could be used to negatively affect employees (a legitimate fear given recent corporate and government data breaches). PII protection policies may include encrypting employee PII, maintaining adequate firewalls and anti-virus software, avoiding use of employee social security numbers as means of employee identification, running an adequate record retention program, and employing measures that ensure business partners who access data also employ similar processes.
- Tools to manage access to data and personal information require the right balance of permissiveness and monitoring, achieved through fostering accountability, continuous training, security procedures (such as user monitoring), and control mechanisms. No matter what the strategy, communicating the intent of both security and privacy-respecting processes will provide people with more confidence in their employers and government. Balanced programs involve monitoring both known threats and user behavior concurrently, so as to quickly inform users to new threats and to augment methods used to assess those threats. This approach will pave the way for a unified approach (both human- and enterprise-focused) to information security.
- Institutions need to foster a cybersecurity mindset that is capable of continually adapting to counter changing threats. This mindset is likely best attained through a leadership-driven cybersecurity culture throughout the enterprise that results in shared "digital trust." Therefore, the responsibility for maintaining this trust not only lies with those in an organization tasked with monitoring information systems (such as that found in a security operations center—SOC—a group within an organization whose mission is to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents with the aid of both technology and well-defined

105 Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, "Deep learning," *Nature 521*, 2015.

106 Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems 29*, 2013.

107 Euijin Choo, Jianchun Jiang, and Ting Yu, "COMPARS: toward an empirical approach for comparing the resilience of reputation systems," *Proceedings of the 4th ACM conference on Data and application security and privacy*, March 3–5, 2014.

108 Timothy Morey, Theodore Theo Forbath, and Allison Schoop, "Customer data: Designing for transparency and trust," *Harvard Business Review 93*, 2015, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

109 Ibid.

processes and procedures), but extends from the top leadership to the entire workforce.[110]

Governments and other organizations that implement insider threat programs should be transparent and make clear to their workforces what types of personnel data and activities they monitor to help identify insider threats with the intent of protecting the workforce, sensitive information, and the viability of the organization itself.

Conclusion

Organizations must place trust in each employee that accesses sensitive data or systems; however, a well-trusting environment does not mean that users have unrestricted access to information or that an institution must accept massive amounts of risk. By analyzing employees' cyber footprints as well as non-IT–based behavioral indicators, organizations may have a more complete picture of potential risks. To ensure a healthy and trusting environment requires that institutions facilitate a cultural norm around security; one that includes high levels of transparency and standardization and that is capable of adapting to evolving threats, including non-human ones.

110 Pierluigi Paganini, "What Is a SOC (Security Operations Center)?" *Security Affairs*, May 24, 2016, http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html.

CHAPTER 3

Big Data: The Latest Tool in Fighting Crime

Benjamin C. Dean

Benjamin C. Dean
President, Iconoclast Tech

A confluence of trends around digital technologies, data collection, and data analysis over the past two decades has brought new opportunities and challenges to public and private organizations alike. Digital technologies and data analysis can and are increasingly used to identify "bad actors" so as to detect and deter or prevent fraud, money laundering, bribery, terrorism, regulatory non-compliance, and other criminal activities. A variety of techniques are now used including profiling, metadata collection, network analysis, data fusion, and predictive analytics. While powerful when used properly, data and data analysis are still subject to statistical and economic limitations. Organizations require people with new skills and a realistic understanding of what these technologies can and cannot do to be able to effectively deploy these technologies and analytical techniques.

After briefly defining relevant terms and outlining trends that have driven advances in digital technologies, this chapter provides an overview of ways in which organizations are taking advantage of advances in digital technologies and data analysis to profile, track, and mitigate malicious actors. Case studies are provided throughout to illustrate the strengths and weaknesses of each of these methods. The final section provides some recommendations based on the issues raised throughout the chapter.

Definitions

"Bad actors" are defined as those individuals or entities whose activities are in contravention of the laws or policies of the United States and other authorities. Examples of such actors include transnational criminal organizations and human traffickers; those conducting financial crimes such as counterfeiting, money laundering, and fraud; terrorists and terrorist organizations; and malicious actors in cyberspace, which encompasses

An illegal diamond dealer from Zimbabwe displays diamonds for sale in Manica, near the border with Zimbabwe. *Photo credit:* Reuters/Goran Tomasevic.

threats emanating from a range of entities—from nation-states to individual actors.[111]

"Digital technologies" are defined as technologies that "fulfil the function of information processing and communication by electronic means, including transmission and display, or use electronic processing to detect, measure and/or record physical phenomena, or to control a physical process."[112] Data, the plural of datum, are information in binary form that can be digitally transmitted or processed.

Technology Trends

Three technological trends related to digital technologies have dovetailed over the past two decades: Faster and cheaper computing power, commonly referred to as Moore's Law, has seen the price of a fixed amount of computing power halved approximately every eighteen months.[113] Network bandwidth has become faster, doubling every nine months.[114] Growing data storage has seen the cost of data storage halved approximately every twelve months.[115]

These technological advances have the potential to create new opportunities for governments and corporations. The adoption of big data analytics has grown in parallel with these advances and has allowed for increased use and experimentation to help increase tax transparency, decrease corruption, counter terrorism, and reduce fraud.

At the same time, these same technologies are also enabling state and non-state actors to promote

111 Department of Defense, *Identity Activities Joint Doctrine,* Note 2-16, August 3, 2016, http://www.dtic.mil/doctrine/notes/jdn2_16.pdf.

112 This is an adaptation of the definition from the Organisation for Economic Co-operation and Development *Glossary of Statistical Terms* (2004) for information and communication technology goods.

113 Ibid.

114 Dan Geer, "Data and Open Source Security," nominal delivery draft for Recorded Future, October 21, 2014.

115 Ibid.

Table 3.1: DoD Categories of Identity Attributes

Biographical	Biological	Behavioral	Reputational
Identity Attribute Sub-Elements			
Core personal Addresses Employment Educational Military service Family Cohabitants Aliases	Individual static Physical attributes (hair/eye color) Scars, marks, tattoos Familial Group Fingerprints, iris, face, palm print, voice, and DNA	Financial transactions Law enforcement records Digital personas Social affiliations Commercial transactions Media consumption/production Body language (gait, posture, eye movements, hand gestures, typing patterns) Micro-expressions (brief involuntary facial expressions)	Judicial judgements Sworn statements Public licenses Financial (historical) Community observations Employer evaluations

Source: DoD, *Identity Activities*.

violent ideologies; obtain and transfer illicit funds; recruit and train personnel; arrange transport, arms, and equipment; and sustain operational communications."[116] The impacts of these crimes can be costly for public and private organizations alike.

Opportunities of Data and Digital Technologies

Advances in digital technologies around collection, analysis, and secure storage over the past two decades have thus simultaneously brought immense opportunities and significant challenges. Many organizations are now taking advantage of advances in digital technologies and data analysis to profile, track, and mitigate malicious actors. This section examines some of the ways in which these technologies and data analysis are being used for this purpose.

Profiling

Profiling is the act or process of extrapolating information about known identity attributes (traits and tendencies) pertaining to an individual, organization, or circumstance.[117] Identity attributes can be categorized in four ways: biographical, biological, behavioral, and reputational.[118] Identity attributes can subsequently be organized into multiple sub-elements to support data collection, analysis, and management. The US Department of Defense (DoD) has developed at least five hundred such data types and sub-types associated with identify attributes (see table 3.1).[119]

If the attributes commonly associated with a particular category of bad actor can be identified, a "signature" (or "fingerprint") can be constructed for that actor. Subjects' profiles can then be compared against this signature to flag potentially undesirable actors and activities.

Box 3.1. The Total Information Awareness Project and Its Ancestors

In 2002, the Information Awareness Office of the Defense Advanced Research Projects Agency (DARPA), led by Dr. John Poindexter, began developing the Total Information Awareness project (later the Terrorism Information Awareness project). The project was premised on the belief that terrorist activity has an information signature.[120] It was hoped that by identifying these signatures, patterns of activity or transactions that

116 Department of Defense, *Identity Activities.*

117 Adapted from the Merriam-Webster Learner's Dictionary full definition of "profiling."

118 Department of Defense, *Identity Activities.*

119 Ibid.

120 John Poindexter remarks, *Overview of the Information Awareness Office*, DARPATech 2002 Conference, Anaheim, California, August 2, 2002, https://fas.org/irp/agency/dod/poindexter.html.

analysts had predetermined were associated with terrorist attacks could be used to scan through databases (containing phone calls, emails, text messages, rental car reservations, credit card transactions, prescription records, etc.) to investigate past terrorist incidents and preempt potential incidents in the future.[121] Profiling by determining which individuals exhibited attributes previously associated with terrorists was considered essential to preempting potential incidents.

Following congressional concerns about the project, linked to privacy issues, the Total Information Awareness project was defunded in 2003.[122] Components of the project were later transferred from DARPA to other government agencies including the Advanced Research and Development Activity.[123] One of these components was the core architecture, later named Basketball, which was described as a "closed-loop, end-to-end prototype system for early warning and decision-making."[124] Another component was Genoa II, later renamed Topsail, which analyzed domestic call metadata to help analysts and policy makers anticipate and preempt terrorist attacks.[125]

Today, the ancestors of these elements of the Total Information Awareness project live on in the counterterrorism-related activities of intelligence agencies, law enforcement authorities, and the private companies that develop these services for public authorities. In spite of long-standing issues with regard to the effectiveness of profiling for counterterrorism purposes, both for methodological[126] and practical[127] reasons, a new generation of machine learning and artificial intelligence techniques is now being applied in the hope of overcoming these prior issues.[128]

Profiling has been used for many decades. Advances in technologies are making it more practical and cheaper to integrate identity attribute data from many sources into a single or multi-layered profile. However, some forms of profiling—by their nature—create privacy and civil liberty concerns. Ensuring that adequate oversight is in place to avoid infringing upon relevant legislation is essential to the success of profiling activities.

Metadata

At the most basic level, metadata are data that provide information about other data, giving people an understanding of what the data constitute. For instance, statisticians use metadata to help data users understand characteristics of data. For survey data, this might include the sample population, the unit of analysis, and the reference period. For a more practical example, when a phone call is made the data can be considered the content of the call itself. The metadata of the call would include the caller, the recipient, the time of the call, and the location of the call.

Metadata are typically divided into the following categories:[129]

- **Descriptive metadata**, which describe a resource for purposes such as discovery and identification, e.g., title, abstract, author, and keywords.
- **Structural metadata**, which indicate how compound objects are put together, e.g., how pages are ordered to form chapters.
- **Administrative metadata**, which provide information to help manage a resource, e.g., the origin of data as well as whether and/or how the data may have been altered. There are several subsets of administrative data; two that are sometimes listed as separate metadata types are *rights management metadata*, which deal with intellectual property rights, and *preservation metadata*, which contain information needed to archive and preserve a resource.

121 Shane Harris, *The Watchers: The Rise of America's Surveillance State* (New York: Penguin Books, 2010).

122 Federation of American Scientists, *Congressional Record: September 24, 2003 (House) H8500-H8550*, 2003, https://fas.org/sgp/congress/2003/tia.html.

123 Mark Williams Pontin, *The Total Information Awareness Project Lives On*, MIT Technology Review, 2006, https://www.technologyreview.com/s/405707/the-total-information-awareness-project-lives-on/.

124 Shane Harris, "TIA Lives On," National Journal, February 23, 2006, https://web.archive.org/web/20110528231531/http://shaneharris.com/magazinestories/tia-lives-on/.

125 Ibid.

126 Jonathan Rae, "Will It Ever Be Possible to Profile the Terrorist?" *Journal of Terrorism Research* 3, no. 2 (2012): DOI: http://doi.org/10.15664/jtr.380.

127 William Press, "Strong Profiling Is Not Mathematically Optimal for Discovering Rare Malfeasors," *Proceedings of the National Academy of Sciences of the United States of America* 106, no. 6 (2008): 1716-1719.

128 Aline Robert, "Big Data Revolutionises Europe's Fight against Terrorism," Euroactiv.fr, June 23, 2016, https://www.euractiv.com/section/digital/news/big-data-revolutionises-europes-fight-against-terrorism/.

129 Jenn Riley, *Understanding Metadata: What Is Metadata, and What Is It For?*, National Information Standards Organization, 2004, http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

Box 3.2. The Panama Papers: Tracking Tax Evasion through Analysis of Large Datasets[130]

In early 2016, a network of journalistic outlets began releasing stories collectively known as the Panama Papers. The stories centered on a law firm, Mossack Fonseca, which had facilitated tax avoidance or evasion for many decades. An unknown person with access to the firm's internal communications began leaking this information to a journalist at the *Süddeutsche Zeitung*. At least 2.6 terabytes of data were leaked.

So overwhelmed was the newspaper that received this enormous amount of data that it enlisted the help of the International Consortium of Journalists, who in turn fed the data to over four hundred other journalists. Entirely new kinds of journalistic teams had to be assembled to secure (e.g., encrypt), scan, index, search, store, order, distribute, edit, and share the data across continents. Making sense out of the data required skills in data visualization and graphics.

Some governments are now using these large databases—and the metadata they contain—to connect the dots and crack down on tax evasion. For instance, Denmark recently paid approximately US$1.3 million for a leaked dataset from the Panama Papers containing information on potential Danish tax evaders.[131]

Metadata are data about data. The metadata associated with data contained in large datasets can be analyzed, and potentially used as inputs to visualizations, to provide an analyst or audience with a better understanding of the contents of a large dataset.

Network Analysis

The origins of network analysis lie in the mid-1700s with Swiss mathematician Leonhard Euler, whose work led to graph theory.[132] In essence, graph theory is concerned with nodes (which could be people, devices, organizations, or other entities) and links between those nodes, which, in sum, represent a network.

Once mapped, a network can be analyzed to determine characteristics of specific nodes, e.g., those that have the most direct connections to other nodes (degree centrality, degree distribution), those that are best connected in the network (betweenness centrality), or those that have best access to the network (closeness centrality). The entire network (or "network topology") can be characterized by how efficiently information can be exchanged (efficiency), the density of links between nodes in a network (modularity), and many other attributes.[133]

After many years of theoretical development, network analysis capabilities were greatly enhanced by technological advances surrounding telephony since the 1980s, computing advancements during and since the 1990s, and the emergence of online social networks in the 2000s. These advances provided both the computational capability and data sources necessary to undertake large-scale network analysis.

Box 3.3. Network Analysis and Mapping Out Criminal or Terrorist Organizations

Much has changed since the 1990s, when Harvard University Professor Malcolm Sparrow lamented that "the concepts of network analysis are highly pertinent to many forms of intelligence analysis and are currently being used seldom, if at all."[134] Spurred-on, in particular, by the overhauling of intelligence activities following the attacks on September 11, 2001, network analysis and metadata collection have been increasingly used as tools for mapping out criminal or terrorist networks and organizations, identifying central individuals, and monitoring communications of individuals in these networks.

One publicly available example of network analysis put into practice for such purposes is a 2002 paper by Valdis Krebs entitled "Mapping of Terrorist Cells."[135] Krebs constructed a network graph—based on publicly available information—of those who hijacked flights on September 11, 2001.

Unfortunately, there is limited publicly available information on the workings of terrorism-related work undertaken by government

130 Information primarily taken from Alan Rusbridger, "Panama: The Hidden Trillions," *New York Review of Books*, Issue 27, October 2016.

131 Glyn Moody, "Panama Papers: Denmark to Pay $1.3M Plus for Leaked Data to Probe Tax Evasion," Ars Technica, September 9, 2016, http://arstechnica.com/tech-policy/2016/09/panama-papers-denmark-payout-data-tax-evasion-probe/.

132 Greg Satell, *How the NSA Uses Social Network Analysis to Map Terrorist Networks*, DigitalTonto, June 12, 2013, http://www.digitaltonto.com/2013/how-the-nsa-uses-social-network-analysis-to-map-terrorist-networks/.

133 Linton C. Freeman, *Centrality in Social Networks: Conceptual Clarification*, *Social Networks* 1 (1978/79): 215-239.

134 Malcolm K. Sparrow, "Application of Network Analysis to Criminal Intelligence," *Social Networks* 13, no. 3 (September 1991): 251-274.

135 Valdis Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24, no. 3 (2001): 43-52.

agencies.[136] One instance that is known is the US National Security Agency's bulk-telephony metadata collection program. This program uses network analysis to identify and link suspect individuals based on metadata collected from their call records.[137] Network analysis methods are also used for social media monitoring, which allows analysts to link profiles associated with terrorist-related content to other profiles that have interacted with the original profile.[138]

The use of metadata and network analysis provides a powerful combination for understanding how entities interact and the emergent behavior networks of entities. Social networks have created a new source of data, and associated metadata, which are used by intelligence and law enforcement agencies in their counterterrorism activities.

Data Fusion

Data fusion describes the process by which several datasets are brought together from multiple sources to create a new, singular dataset. The Joint Directors of Laboratories, which pioneered a multi-level data fusion model in the early 1990s, defines data fusion as a "multi-level, multifaceted process handling the automatic detection, association, correlation, estimation, and combination of data and information from several sources."[139]

The advantages of data fusion mainly involve enhancements in data authenticity or availability.[140]

The field of data fusion has developed to address four broad challenges associated with data inputs: data imperfection, data correlation, data inconsistency, and disparateness of data form.[141] Different algorithms are used to address these varying challenges. No single data fusion algorithm is capable of addressing all of them.

Different combinations of these challenges will arise depending on the use case in question due to the various data inputs being used. It is crucial to identify which of these challenges may be present up-front because, if they are not rectified, any error introduced will be magnified in later output.[142]

Predictive Analytics and Machine Learning

Predicative analytics uses statistical techniques to derive a probabilistic score for the likelihood an entity will perform a given action in the future. The analysis is typically based on its current and past profile attributes relative to a comparable population.

In the past, regression techniques have been a mainstay of predictive analytics. Regression involves determining a relationship (correlation) between a dependent variable and an independent variable in a given population. There are many regression models (e.g., linear, logistic, probit) that might be used depending on the phenomenon under examination.

In recent years, machine learning techniques have become increasingly popular for predictive analytics. Machine learning involves the application of induction algorithms, which intake specific instances and produce a model that generalizes beyond those instances.[143] Rather than program a computer to perform a certain task, machine learning involves inputting data into an algorithm that then leads the computer to change its analysis technique.

There are two broad categories of machine learning algorithms: supervised and unsupervised. The former uses labelled records to sort data inputs into known outputs. The latter does not use labelled records so the outputs are not known ex ante. The algorithm explores data, finds some structure, then uses this to determine the outputs. This is particularly useful for use cases like fraud detection or malicious network activity, where the phenomenon to be detected is too rare or its outward characteristics are unknown. Unsupervised learning algorithms are better at searching for anomalies, which signal significant deviation from some sort of "normal."

Machine learning and other more advanced analytical techniques have been deployed for many years to assess consumer credit[144] and detect credit

136 Steve Ressler, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," *Homeland Security Affairs* 2, Article 8 (July 2006), https://www.hsaj.org/articles/171.

137 "Documents on NSA Efforts to Diagram Social Networks of US Citizens," *New York Times*, September 28, 2013, http://www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html.

138 Ibid.

139 F.E. White, Data Fusion Lexicon, Joint Directors of Laboratories, Technical Panel for C3, Data Fusion Sub-Panel, Naval Ocean Systems Center, San Diego, California, 1991.

140 Bahador Khaleghia, Alaa Khamisa, Fakhreddine O. Karraya, and Saiedeh N. Razavi, "Multisensor Data Fusion: A Review of the State-of-the-Art," *Information Fusion* 14, no. 1 (2013): 28-44.

141 Ibid.

142 With thanks to Daniel Meisner, senior director, Platform, head of Open Data and Ecosystems, Thomson Reuters, for pointing this out.

143 Ron Kohavi and Foster Provost, "Glossary of Terms," *Machine Learning* 30 (1998): 271–274, http://ai.stanford.edu/~ronnyk/glossary.html.

144 Amir E. Khandani, Adlar J. Kim, and Andrew W. Lo, "Consumer Credit Risk Models via Machine-Learning Algorithms," MIT

card fraud.[145] Such practices, previously also used in matchmaking on online dating sites, are now beginning to find applications in such varied areas as graduate recruitment.[146]

Box 3.4. Use of Predictive Analytical Techniques to Improve Policing Outcomes

The field of predictive policing seeks to use advances in data collection and analysis to identify instances of increased crime risk and develop/deploy an associated prevention strategy to mitigate and/or reduce those risks.[147] Varying levels of success for these initiatives have been observed; the extent of success has been linked in part to the specific use case, the phenomena under examination, and the relative operational capabilities and resources of the law enforcement agency in question.

One study[148] used a randomized controlled field trial to evaluate the effectiveness of an Epidemic Type Aftershock Sequence (ETAS) crime forecasting model as compared with the existing best practice used by crime analysts in a district.[149] Trials were held with the Los Angeles Police Department (United States), where analysts traditionally used a COMPSTAT (computer statistics) policing model, and with the Kent Police Department (United Kingdom), where analysts traditionally used an intelligence-led policing approach.

Overall, the study found that ETAS models outperformed analysts' and their traditional techniques. For instance, in the United Kingdom (UK), the analyst predicted 6.8 percent (Maidstone, England) and 4.0 percent (Sevenoaks, England) of crimes successfully compared with 9.8 percent and 6.8 percent, respectively, by the ETAS model. In the United States, the analyst successfully predicted 2.1 percent of crimes compared with 4.7 percent for the ETAS model. Relative to the amount of patrol time allocated to certain hotspots, ETAS-predicted locations were expected to experience 7.4 percent fewer crimes (on a mean of 58.17 crimes per division) per week in the absence of patrol. Analysts' use of traditional methods was expected to yield half the reduction (~3.7 percent) at equivalent patrol levels.

Another study[150] evaluated the effectiveness of the first version of the Chicago Police Department's Strategic Subject List (SSL) predictive policing program. The program's goal was to use social network analysis methods to identify people at risk of gun violence. These people were then to be referred to local police commanders for preventive intervention in the hopes of reducing future crimes linked to gun violence.

The predictive model ended up identifying only 1 percent of the eventual homicide victims (3 out of 405 victims). The program did, however, result in SSL subjects being more likely to be arrested for a shooting.[151] This last finding was thought to indicate that the police used the list as a resource to pursue criminals after the fact, rather than in accordance with the intended purpose: to intervene before crimes took place. The lesson to acknowledge from this case is that the outcomes from using technology, like predictive analysis, will be only as good as the organizational arrangements that allow insights to be acted upon appropriately.

Machine learning techniques have become increasingly popular for predictive analytics. Unsupervised learning algorithms in particular allow for the identification of rare phenomena that may previously have been difficult to identify in large datasets. As with any technology, one key to

Sloan School of Management and Laboratory for Financial Engineering, 2010, https://dspace.mit.edu/openaccess-disseminate/1721.1/66301.

145 Richard J. Bolton and David J. Hand, "Unsupervised Profiling Methods for Fraud Detection," Imperial College, London, via CiteSeerX, 2001, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.24.5743.

146 Laura Noonan, "Deutsche Uses Koru's 'Dating Site' Tech to Enhance Match with New Recruits," *Financial Times,* September 7, 2016, https://www.ft.com/content/b83108fe-72b4-11e6-bf48-b372cdb1043a.

147 Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith, and John S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Rand Corporation, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

148 G. O. Mohler, M. B. Short, Sean Malinkowski, Mark Johnson, G. E. Tita, Andrea L. Bertozzi, and P. J. Brantingham, "Randomized Controlled Field Trials of Predictive Policing," *Journal of the American Statistical Association* (2015): DOI: 10.10.1080/01621459.2015.1077710.

149 ETAS models are analogous to those used for seismic activity. Using an Expectation-Maximization algorithm, as crimes occur in real time, the model adjusts the probabilities of future crime hotspots similar to the way that one might model aftershocks following an earthquake (if one incident occurs in a hotspot, it is more likely that others will follow).

150 Jessica Saunders, Priscilla Hunt, and John S. Hollywood, "Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot," *Journal of Experimental Criminology* 12, no. 3 (September 2016): 347–371, DOI 10.1007/s11292-016-9272-0.

151 Ibid.

effectively using predictive analytics is having the appropriate organizational measures in place to act upon the insights gleaned from these techniques.

Blockchain

One of the most interesting and groundbreaking technological innovations of the past decade is the blockchain that underpins bitcoin, a digital currency supported by cryptographic methods (a "cryptocurrency"). One of the key technologies that secures bitcoin is a distributed, publicly available, and immutable ledger commonly referred to as a blockchain.

In very simple terms, a blockchain is a shared database with time-stamped entries. The name is derived from the way in which transactions are grouped together (into a block) and added to the ledger sequentially. Each block is linked to the previous block, thereby making a chain (hence, "blockchain"). That the entries form a chain allows anyone to trace back through the history of transactions to see and confirm what transactions took place between whom and at what time. Three broad types of blockchains have emerged—public, private, and a hybrid of the two.[152] They are differentiated based on their level of centralization/decentralization, their consensus mechanism, and who has read or write ability.

A blockchain is used in bitcoin to prevent the double-spend problem. Before bitcoin, the issue with a digital currency was that someone could spend the same unit of digital currency in multiple places at the same time. A blockchain solves this problem by providing a shared ledger, which ensures that everyone knows and agrees on how much of the digital currency has transacted among users at any point in time.

It is thought that blockchains might provide an effective tool in detecting and preventing corrupt or fraudulent activities. This thinking is premised on the immutability of a blockchain. The immutability prevents any one party from altering past entries, as one might be able to do with paper or digital records.

Box 3.5. Using Blockchain to Address Fraud and Theft

Everledger is a UK-based company that uses public and private blockchains, along with other technologies, to address a novel problem: diamond theft and associated insurance fraud. This problem stems from two factors. First, there previously was not a dependable way to detect if a diamond had been stolen. Moreover, like other luxury goods, proof of ownership remains on paper documents, which are vulnerable to tampering and loss.[153]

Everledger creates a unique, digital "thumbprint" of a diamond, which records its individual set of attributes including color, clarity, cut, and carat weight, as well as forty other metadata points, and links these to the laser inscriptions on the girdle of the stone.[154] It then places this information on the blockchain to create an immutable entry. If stolen, the diamond's original owner can be traced using this entry on the blockchain.

As many organizations that are experimenting with blockchain have found out, there are inherent difficulties using a technology designed to track digital currency transactions for other use cases. Attempting to register physical assets using a digital entry on a blockchain requires a trusted third party. However, bitcoin was designed specifically to remove the need for such a trusted third party through a computationally intensive consensus mechanism.[155] Trust in Everledger therefore becomes paramount, as opposed to bitcoin, where trust is intentionally factored out by design.

Moreover, placing information on any public blockchain—such as the bitcoin blockchain—necessitates making that information publicly available. This might not be appropriate for some sensitive or private information. To overcome this, Everledger uses a private blockchain, with sensitive data such as police reports and policy information kept on the company's Eris-run platform.[156]

152 Vitalik Buterin, "On Public and Private Blockchains," Ethereum Blog, August 7, 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

153 Grace Caffyn, "Everledger Brings Blockchain Tech to Fight against Diamond Theft," CoinDesk, August 1, 2015, http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft/.

154 "On Blockchain, Diamonds Are Forever," Rakuten Today, October 4, 2016, https://rakuten.today/blog/everledger-blockchain-diamonds-forever.html.

155 Steve Wilson, "Blockchain Plain and Simple," Constellation Research, January 30, 2017, https://www.constellationr.com/blog-news/blockchain-plain-and-simple.

156 Grace Caffyn, "Everledger Brings Blockchain Tech to Fight against Diamond Theft."

The bitcoin blockchain has inspired numerous new projects that all seek to build on the cryptocurrency's original success. However, it must be remembered that the bitcoin blockchain was developed to solve one very specific problem: double-spend. As new projects continue to develop, such as Hyperledger and Ethereum, many new possibilities for applications of distributed/shared ledger technology will emerge.[157]

Shortcomings and Limitations of Data and Digital Technologies

Although the cost of profiling and data fusion are falling due to Moore's Law and other technological advances, there are important economic, statistical, and practical/operational issues that commonly stand in the way of effective deployment of these technologies. As with any tool, use of big data methods will be effective only if those who wield these tools have the requisite knowledge of their applications and shortcomings.

Privacy Considerations

Strict privacy-related laws have been in place for many decades, in the United States and abroad, to constrain the ability of public and private sector organizations to collect and use personal data. In particular, the European Union's General Data Protection Regulation, which will come into effect in 2018, has specific clauses related to practices such as profiling.

As some of the case studies throughout this chapter have illustrated, large-scale data collection and analysis can often fall foul of privacy laws.

Part of the issue is that anonymized data can be de-anonymized when several data sources are combined.[158] Likewise, non-personally identifiable information can become personally identifiable information—which is treated differently legally—when combined with other data.[159]

A privacy assessment is therefore essential to any initiative using large-scale data collection and analysis to avoid infringing upon privacy laws and civil liberties.

False Positives and Negatives

An important limitation of any profiling effort across relatively large populations is the occurrence of false positives and false negatives. A false positive can be thought of as a false alarm. According to New York University's distinguished professor of risk engineering, Nassim Nicholas Taleb, the "tragedy of big data" is that even though one has more data, it also means one has more false information.[160] More false information makes it harder, and costlier, to correctly identify the desired targets. Reducing the incidence of false positives or negatives becomes more costly as one attempts to eliminate such errors from the predictive analysis.

"... [U]se of big data methods will be effective only if those who wield these tools have the requisite knowledge of their applications and shortcomings."

This may not be an issue in cases where incorrectly identifying and acting upon an entity that is a false positive does not result in enormously meaningful repercussions.[161] However, in instances where there are meaningful repercussions from such an error, the benefits of such predictive profiling may be (substantially) outweighed by the costs.

The Unit of Analysis with Dynamic Profiles in Heterogeneous Populations

The first step in profiling is determining what the unit of analysis should be. In other words, "What do we watch—the farmer, the dog, the chickens, or the coop"?[162] The answer to this question may not immediately be obvious. If the correct unit of analysis is not chosen, however, the rest of the profiling exercise—and the output of any subsequent analysis—is moot.

Moreover, profile attributes are dynamic—they are shaped by many inputs over time and as such can shift depending on the changing circumstances. The true rates of bad actors, which are sentient and

157 See "About the Hyperledger Project," Hyperledger, https://www.hyperledger.org/about and Ethereum, https://www.ethereum.org/, for more information.

158 Latanya Sweeney, "K-anonymity: A Model for Protecting Privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems* 10, no. 5, (2002): 557-570.

159 Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 (2010): 1701.

160 Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder* (New York: Random House, 2012).

161 Daniel Geer, *Measuring Security*, Tutorial, 2007, v2.1:16x07, http://geer.tinho.net/measuringsecurity.tutorial.pdf.

162 Ibid.

thus able to adapt, might also change over time. All these elements require data inputs to be continually tracked and updated, which might not be cheap or practical.

Effective Interpretation of Results and Intervention Strategy

While robust and extensive data analysis might be undertaken with cutting-edge predictive analytic methods, this does not imply that the results of such analysis will subsequently be correctly interpreted and acted upon. There are inherent limitations in using these techniques, and not fully understanding them can have consequences. This is particularly the case when attempting to measure or identify a person's emotions or state of mind.[163]

Even in cases where the analysis is correctly interpreted and understood, an effective prevention or intervention strategy must be developed and deployed to mitigate the identified risk(s).[164] However, the history of predictive policing suggests that developing and deploying these strategies is one of the biggest challenges that initiatives using such data analysis techniques face.

Box 3.6. Gouré, Kellan, and RAND's Vietnam Motivation and Morale Project[165]

During the Vietnam War, to understand whether the US-led carpet bombing campaign was reducing the morale of the Vietcong fighters and North Vietnamese citizens, the RAND Corporation extensively interviewed North Vietnamese prisoners and defectors. Starting in 1964, the original leader of the RAND project, Leon Gouré, interpreted from the sixty-one thousand pages of extensive data collection and analysis (the big data of its day) that the bombing campaign was successful (i.e., the Vietcong's morale was falling). One of his colleagues, Konrad Kellan, later reviewed the interviews in 1965. Kellan postulated a different interpretation, concluding that the opposite (and ultimately correct) outcome was occurring, namely, that the bombing campaign only reinforced the morale of the Vietcong and citizens of North Vietnam.[166]

Kellan attributed his key insight, which allowed him to correctly interpret the body of data, to one interview with a senior Vietcong captain:

> He was asked very early in the interview if he thought the Vietcong could win the war, and he said no. But pages later, he was asked if he thought that the US could win the war, and he said no. The second answer profoundly changes the meaning of the first. He didn't think in terms of winning or losing at all, which is a very different proposition. An enemy who is indifferent to the outcome of a battle is the most dangerous enemy of all.[167]

This reality was something that Gouré had overlooked given his own personal history and biases. The lesson here is that while a large body of data might be available, correctly interpreting the data is an entirely different matter. This has not changed in spite of decades of advances in analytical techniques.

Recommendations

A number of lessons on how to successfully deploy digital technologies and data analytics emerge from the various cases covered in this chapter. These lessons form the basis for the recommendations below.

- Invest in people with the skills and knowledge: A broad skill set is required to correctly secure, scan, index, search, store, order, distribute, and edit data as well as visualize/communicate findings from data analysis. Very rarely does any one person possess all of these skills, so multidisciplinary teams must be formed to successfully use digital technologies and data analysis. Organizations should take this into account when considering the adoption and subsequent use of these technologies.
- Ask whether data analysis is appropriate for answering the desired question: Digital technologies and data analysis are relatively better suited to solving some problems, such as optimization, than others, particularly

163 Malcom Gladwell, "Revisionist History: Saigon, 1965, Podcast Episode 2," 2016, based on Gladwell, "Viewpoint: Could One Man Have Shortened the Vietnam War?" BBC.com, 2013, http://www.webcitation.org/6I1RnuJsR.

164 Perry, McInnis, Price, Smith, and Hollywood, *Predictive Policing*; Greg Ridgeway, "Linking Prediction and Prevention," *Criminology and Public Policy* 12, no. 3 (2013): 545-550; Saunders, Hunt, and Hollywood, "Predictions Put into Practice."

165 Gladwell, "Revisionist History: Saigon, 1965, Podcast Episode 2."

166 Gladwell, "Revisionist History: Saigon, 1965, Podcast Episode 2." It is also worth noting that during the Vietnam War, US Secretary of Defense Robert McNamara became blinded to the reality in the field due to his overreliance on data collection and interpretation. In particular, his focus on the body count blinded him to the other—more important—indicators that the war was not winnable. See Kenneth Cukier and Viktor Mayer-Schönberger, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Eamon Dolan/Mariner Books: 2013). The same methods that worked well in reducing the costs of Ford motorcar production ended up disastrous for the conduct of full-scale war in Vietnam—another lesson that applying effective techniques from one use case does not mean success will occur for other use cases.

167 Gladwell, "Revisionist History: Saigon, 1965, Podcast Episode 2."

those involving behavior or emotions. Before embarking on a data analysis exercise to answer a question, organizations first need to consider whether the techniques they intend on using will be able to generate useful answers. This recommendation also applies to blockchains. Organizations need to consider whether an immutable, publicly available database that requires immense computing power to maintain consensus is superior—given the use case—to relatively more simple, long-standing options in the field of distributed databases.

- Place technology use within a larger strategy: Even if data analysis is correctly done and the results are correctly interpreted and then communicated, the exercise becomes moot if there is not robust implementation/operationalization of the results. Organizations need to understand technology use and data analysis not in isolation but as part of a wider organizational strategy.
- When investing in data analysis technologies, consider all available options: Many data analysis technologies and databases or data sources are open source and freely available. However, in some cases, a custom-built "data analysis solution" might be needed to accomplish organizational goals.
- More data do not necessarily equal better data: A common misconception is that collecting and adding more data results in "better" data. The issue is that beyond a certain point, more data tend to create more noise, which results in "worse" data. Organizations need to consider how much data are required to answer the question they have and determine at what point sufficient data have been collected for useful analysis to be undertaken.

Conclusion

Digital technologies and data analysis have advanced greatly over the past two decades. A variety of techniques are now available including profiling, metadata collection, network analysis, data fusion, and predictive analytics. These techniques can be, and increasingly are, used to profile and track bad actors to detect and deter or prevent fraud, money laundering, bribery, terrorism, and regulatory non-compliance. While powerful when used properly, these technologies are most effective when deployed by organizations in which the staff have appropriate skills and a realistic understanding of just what benefits the technologies can provide.

CHAPTER 4

Big Data: Tackling Illicit Financial Flows

Tatiana Tropina

Tatiana Tropina
Senior Researcher, Max Planck Institute for Foreign and International Criminal Law

The relatively new phenomenon of big data has rapidly become both a promise and a challenge. Big data solutions are praised by some as technologies that will change the world, criticized by others as threats to privacy, acclaimed to be a silver bullet to myriad issues, called a "buzzword tsunami," and used as a source of inspiration for utopian and dystopian scenarios; big data has quickly become central to many policy debates. Governments, law enforcement agencies, and the private sector are currently trying to grasp the benefits of the huge amounts of data generated and processed daily and exploring how big data can help them perform better in different areas—from healthcare to preventive policing and from targeted advertising to research and innovation, to name but a few. Meanwhile, criminals strive to use big data to their advantage as well.

There is still no agreed-upon definition of big data, though many define it as the rapidly increasing production, storage, and transfer of large amounts of data available from different sources, along with the algorithms and tools needed to process them. However, though its definition is still being debated, big data is already a reality. Despite ongoing debates around the use of big data tools for preventing and controlling crime, there is no question "if" these tools will be employed: the questions are only "how" and "when." There is also little doubt that, once implemented properly, big data analytics can be revolutionary in tackling illicit financial flows.

This chapter explores both how big data is used by criminals to create illicit profits and how law enforcement and other institutions can use big data to help tackle this problem. It begins with a brief explanation of the concept of illicit financial flows and examination of how digital technologies are changing the face of online and offline profit-driven crime. It also investigates the promises and challenges of using big data to stop illicit financial flows and discusses the balance between law and technology required to address the problem of illegally acquired money. Finally, recommendations highlight the need for long-term approaches to

combat the problem of crime, wherein big data and other technological solutions should be made part of comprehensive strategies.

Digital Technologies and Illicit Financial Flows: State of Play and Possible Developments in the Era of Big Data

In the past few years, use of the term "illicit financial flows" has grown; these illegal flows are now a crosscutting issue on the agenda of governments and international organizations such as the World Bank and Organisation for Economic Co-operation and Development (OECD), amongst others. Despite a lack of consensus regarding the extent to which this term covers grey areas and practices such as tax avoidance, the general understanding is that it refers to money "illegally earned, transferred or used."[168] The notion of illicit financial flows aims to connect seemingly disparate illegal activities under a single umbrella to tackle the whole lifecycle of illicit finance—from earning to utilization—and provide a holistic picture of the issue. The umbrella approach makes even more sense in the digital age, where technology has increasingly become a common enabler. It also makes it possible to adopt harmonized frameworks to trace illegal money, to share best practices between regulatory domains, and, ultimately, to connect previously fragmented efforts.

The legal and technical solutions for tracing crime in a digital environment have never been perfect, and in an age of exponentially increasing data, finding solutions is now akin to finding the proverbial needle in a growing haystack of data. However, big data also makes it easier to trace criminal activity.

Illicit Profits: How Digital Technologies Are Changing the Face of Crime

As information and communications networks have changed the way of doing business and the manner of social interactions, they have also been employed by criminals to both facilitate traditional criminal activities and enable new types of crimes.

Box 4.1. Underground Economy of Cybercrime: Automation and Botnets

Automation plays a vital role in the functioning of the underground economy: without it criminals would have to manually target individual victims and computer systems, thus making attacks and crimes too costly and time consuming. The core of automation and the backbone of the underground economy are the botnets, i.e., networks of compromised computers that can be remotely controlled by the perpetrators and used as "zombies" to launch large-scale denial-of-service attacks on computer systems, disseminate malware, and look for system vulnerabilities. Trading botnets is a very profitable activity in the "crime as service" business model, which is based on offering services, such as hacking and carding, and tools to commit cybercrime for sale or rent. Botnets are offered at a low cost relative to profit due to the high volume of "customers" and overall turnover: distributed denial-of-service attacks can be purchased for $10 to $1,000 per day.[169]

The Digital Underground Economy

Cybercrime, which in the last decade has transformed into a complex and thriving digital underground economy, is one of the most direct links between digital technologies and illicit financial flows. This economy is based on the monetary value of data as an illegal commodity,[170] which is moved across national borders and traded in underground online marketplaces.[171]

Technological developments are transforming both the legitimate and illicit economies, in part by decentralizing operations as value chains are being replaced with value networks. The patterns of doing business in criminal ecosystems bear many similarities to legitimate business-to-business models regarding decentralization, product placement, outsourcing, subcontracting, and networking. And, like legitimate businesses, those in the criminal economy strive to profit from the development of new business models based on the use of information, communications technologies,

168 United Nations Economic Commission for Africa, Report of the High Level Panel on Illicit Financial Flows from Africa, 2015, http://www.uneca.org/sites/default/files/PublicationFiles/iff_main_report_26feb_en.pdf; see also "Illicit Financial Flows (IFFs)," World Bank, 2015, http://www.worldbank.org/en/topic/financialmarketintegrity/brief/illicit-financial-flows-iffs.

169 Europol, Threat Assessment: Internet Facilitated Organized Crime, The Internet Organised Crime Threat Assessment, File No.: 2530–264, The Hague, January 7, 2011, https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf; see also Candid Wueest, "Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services," Symantec Official Blog, November 20, 2015, http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

170 For example, according to SecureWorks, in 2015-2016 the price for stolen credit card credentials varied from $4–$80 per item, the price for stolen online payment account credentials varied from $20 to $149 per item depending on the account balance, and the full packages of identity information were traded for $15–$65. See Dell, SecureWorks, Underground Hacker Markets, Annual Report – April 2016, http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf.

171 Hanno Fallmann, Gilbert Wondracek, and Christian Platzer, "Covertly Probing Underground Economy Marketplaces," Vienna University of Technology Secure Systems Lab, 2010, http://www.iseclab.org/papers/dimva2010_underground.pdf; Europol, The Internet Organized Crime Threat Assessment (iOCTA), 2014, https://www.eurssopol.europa.eu/content/internet-organized-crime-threat-assesment-iocta.

and analysis of digital data. These new models allow money stolen through cybercrime to generate illicit revenues, from the supply of the tools to the commission of the crimes. Highly sophisticated criminal-to-criminal services offer "crime as service" tools, including training tutorials, while making them available for "customer" demand at relatively low prices compared with the potential illicit profits.[172]

Information Technology as a New Tool for 'Traditional' Organized Crime

Criminal organizations carrying out "traditional" illegal activities use digital tools for planning and coordination, communications, networking, and trading illegal goods, including arms, drugs, and counterfeit documents. The Internet merges these activities with those related to cybercrime—such as the trade in botnets and tools to commit digital crimes and trade in stolen personal data—and outsources the commission of digital crimes. These two trends drive the creation of online criminal hubs—hidden online marketplaces—where the trade of traditional illegal goods and services coexists in the "darknet" with the supply of tools to commit cybercrimes.

A trend that is distinct from using the Internet to facilitate the trade of illegal goods, and much more worrisome, is the attempt by traditional organized crime groups to employ the skills of highly qualified cybercriminals to carry out the sophisticated manipulation of computer systems to facilitate illegal operations. One of the first studied cases of such synergy was discovered in June 2013, when law enforcement agencies detected a Netherlands-based drug smuggling ring that collaborated with hackers to penetrate the systems controlling the movement and location of shipping containers and—as a result of data manipulation—was able to collect cargos with drugs before the legitimate carrier was able to get them.[173]

Terrorist Financing

The Internet is a well-known vehicle for terrorist financing. Terrorist organizations use digital tools and communications technologies to solicit donations and conduct e-commerce schemes for selling books and promotional material to supporters. For example, a group of Islamic State of Iraq and al-Sham militants from Russia has used the very popular digital wallet QIWI to collect money online.[174]

A growing trend concerns the use of digital currencies for terrorist financing: their relative anonymity, ease of use, accessibility, and the fact that they are decentralized and mostly unregulated make them attractive means of carrying out fundraising campaigns. Some of the anti-money laundering bodies—both nationally and internationally—are discussing potential regulatory responses to the possible use of virtual currencies by terrorists. For example, the Financial Crimes Enforcement Network (FinCEN), an agency of the US Treasury Department, is considering establishing a "meaningful regulatory framework for virtual currencies that intersect with the U.S. financial system."[175] In addition, the intergovernmental Financial Action Task Force monitors emerging regulatory issues arising from terrorist financing risks associated with virtual currencies.[176]

Meanwhile, there have already been cases of terrorist organization websites requesting donations via bitcoin.[177] Social media and crowdfunding—whether being used under false pretensions or not—have also emerged as valuable fundraising tools for terrorists.[178] Terrorist organizations and radicalized individuals can also use peer-to-peer lending.[179] Since many of these opportunities use payment methods that exist outside of regulatory oversight and anti-terrorist financing compliance procedures, there is a risk that terrorist networks can use

172 Yuval Ben-Itzhak, "The Cybercrime 2.0 Evolution," ISSA Journal, June 2008, http://professor.unisinos.br/llemes/Aula01/CybercrimeEvolution; Tatiana Tropina, "Organized Crime in Cyberspace" in Heinrich-Böll-Stiftung and Regine Schönenberg (eds.), Transnational Organized Crime: Analyses of a Global Challenge to Democracy, Bielefeld, Transcript Verlag, 2013, 47-60.

173 Europol, iOCTA.

174 Joanna Paraszczuk, "IS Militants Use Popular Russian Web Payment System to Raise Cash," Radio Free Europe, May, 17, 2015, http://www.rferl.org/a/islamic-state-funding-russian-web-payments-qiwi/27021379.html.

175 FinCEN, *Statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, United States Department of the Treasury,* November 19, 2013, https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network.

176 Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach: Virtual Currencies*, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

177 FATF, Emerging Terrorist Financing Risks, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf, 36.

178 Sam Rubenfeld, "Foreign Terror-Fighters Fundraise on Social Media, Crowdfunding Sites," Wall Street Journal, October 21, 2015, http://blogs.wsj.com/riskandcompliance/2015/10/21/foreign-terror-fighters-fundraise-on-social-media-crowdfunding-sites/; FATF, Emerging Terrorist Financing Risks, 31-32.

179 Such concerns were especially raised after it became known that Syed Rizwan Farook, one of the two shooters responsible for the terrorist attack in San Bernardino, California, on December 2, 2015, was able to get a loan of $28,500 through an online peer-to-peer lending website (see, e.g., Darrell Delamaide "Loan to Terror Couple Challenges Regulators," USA Today, December 15, 2015, http://www.usatoday.com/story/money/2015/12/15/shooting-terrorism-online-loans-san-bernardino/77358520/).

virtually any such payment and fundraising tool to their benefit.

Box 4.2. Use of Bitcoin for Terrorist Financing: Ibn Taymiyya Media Center

The case of the Ibn Taymiyya Media Center (ITMC)—an online jihadist propaganda unit located in the Gaza Strip—using bitcoin for fundraising was brought by Yaya J. Fanusie, a former counterterrorism analyst for the US Central Intelligence Agency. According to Fanusie, the ITMC used social media tools to carry out the fundraising campaign in bitcoin. This was the first known case of the terrorist group publicly seeking donations in digital currency. The terrorist unit posted the information on Twitter with QR (Quick Response) codes that were linked to a bitcoin address, which received two bitcoin donations in July 2016.[180]

Tax Fraud, Tax Evasion, and Information Technologies: The Challenges of the Digital Economy

While it is hard to assume that the use of global communications networks has no effect on tax evasion, it is unknown whether there are any specific digital tools employed in this area that help carry out large-scale corporate tax evasion. Undoubtedly, the digital economy and borderless Internet, while enabling operations worldwide, create loopholes in taxation. The possibility that tax bases are becoming severely eroded in the digital economy has prompted international organizations to place this issue on their agendas; the OECD, for example, is currently developing action plans to address the problems associated with taxation in the digital era.[181]

There is, however, a growing synergy between identity-theft cybercrimes and tax fraud. Stolen identities can be used to file tax returns: such schemes involve reporting inflated amounts of income and taxes, and, therefore, claiming inflated tax refunds. Criminals can further seek to transfer these tax refunds to prepaid debit cards.[182]

Use of Information Technologies in Illegal Money Transfers and Integration

Digital tools have significantly transformed many components of illicit financial flows, including the transfer and integration of ill-gotten gains. All stages of money laundering—placement, layering, and integration[183]—are affected by the myriad ways online transactions can be used to distance any type of illicit funds from the source of illegal profit.

Technology does not care about the source of illegal income. The same tools and digital technologies can be used to transfer illicit money of any origin, including from corruption, embezzlement, organized crime, tax evasion, and many other activities. The only difference between online and offline criminal activities for money transfers is that the profits gained from digital crime already exist in the digital environment, so money laundering's risky placement stage can be avoided.[184] The same is true for the illegal trade of goods online in digital currencies: the money is "pre-laundered" because it is placed in mostly unregulated financial institutions.[185]

The countless opportunities for digital transactions via various electronic payment intermediaries—such as transfers from one intermediary to another, peer-to-peer transactions, and transfers to and from the traditional banking system—are making the ecosystem extremely complex[186] and creating obstacles in the identification of suspicious transactions.[187] Many electronic payment intermediaries are less regulated than traditional financial institutions or not regulated at all.[188] Thus, compliance with anti-money laundering laws and the identification of suspicious transactions are left to the unregulated payment intermediary, many of which lack the incentive to detect suspicious

180 Yaya Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," The Cipher Brief, August 24, 2016, https://www.thecipherbrief.com/column/private-sector/new-frontier-terror-fundraising-bitcoin-1089.

181 OECD, Addressing the Tax Challenges of the Digital Economy, OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, 2014, http://www.oecd.org/ctp/tax-challenges-digital-economy-discussion-draft-march-2014.pdf.

182 Internal Revenue Service, *IRS Intensifies Work on Identity Theft and Refund Fraud; Criminal Investigation Enforcement Actions Underway across the Nation,* 2014, https://www.irs.gov/uac/newsroom/irs-intensifies-work-on-identity-theft-and-refund-fraud-criminal-investigation-enforcement-actions-underway-across-the-nation.

183 Key definitions: Placement—depositing money into the financial system, layering—distancing money from its source through a series of transactions, and integration—the commingling of money with funds in legal sectors.

184 Wojciech Filipkowski, "Cyber Laundering: An Analysis of Typology and Techniques," International Journal of Criminal Justice Sciences (IJCJS) 3, no. 1 (2008): 15-27.

185 National Drug Intelligence Center, Money Laundering in Digital Currencies, US Department of Justice, 2008, http://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf.

186 Tatiana Tropina, "Fighting Money Laundering in the Age of Online Banking, Virtual Currencies and Internet Gambling," ERA Forum 15, no. 1 (June 2014): 69-84.

187 Council of Europe, Criminal Money Flows on the Internet: Methods, Trends, and Multi-stakeholder Counteraction, Moneyval Research Report, March 2012, http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf, 36.

188 FATF, Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems, 2008, http://www.fatf-gafi.org/.

A woman looks at a map showing where eight members belonging to a New York-based cell of a global cyber criminal organization withdrew money from ATM machines. The US government charged eight individuals with using data obtained by hacking into two credit card processors in a worldwide scheme that netted some $45 million within hours, a crime prosecutors described as one of the biggest bank heists in history. *Photo credit:* Reuters/Lucas Jackson.

behavior, especially if their primary goal is to provide bulletproof payment services.

The following tools can be used to facilitate illicit financial flows: online banking[189] and mobile banking;[190] electronic payment systems via unregulated financial intermediaries;[191] cryptocurrencies;[192] online services and trading

189 Council of Europe, Criminal Money Flows on the Internet; see also Christine Victoria Thomason, "How Has the Establishment of the Internet Changed the Ways in Which Offenders Launder Their Dirty Money?" Internet Journal of Criminology, July 2009, http://www.internetjournalofcriminology.com/Thomason_Internet_Money_Laundering_July_09.pdf and Stephen J. Weaver, "Modern Day Money Laundering: Does the Solution Exist in an Expansive System of Monitoring and Record Keeping Regulations?" Annual Review of Banking & Financial Law 24, 2005: 443-465.

190 John Villasenor, Christopher Bronk, and Cody Monk, Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-Peer Networks, and Mobile Device Payments, The Brookings Institution and the James A. Baker III Institute for Public Policy, August 29, 2011, http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf. See also LIRNEasia & UP–NCPAG, Mobile Banking, Mobile Money and Telecommunication Regulations, 2008, http://lirneasia.net/wp-content/uploads/2008/05/Mobile-2.0_Final_Hor_EA.pdf.

191 Jean-Loup Richet, Laundering Money Online: A Review of Cybercriminals Methods: Tools and Resources for Anti-corruption Knowledge, United Nations Office on Drugs and Crime, June 1, 2013, arxiv.org/pdf/1310.2368; see also Giulio Piller and Elvis Zaccariotto, "Cyber-Laundering: The Union between New Electronic Payment Systems and Criminal Organizations," Transition Studies Review 16, no. 1 (2009): 62-76, and Tropina, "Fighting Money Laundering in the Age of Online Banking."

192 Danton Bryans, "Bitcoin and Money Laundering: Mining for an Effective Solution," Indiana Law Journal 89, August 29, 2013, http://ssrn.com/abstract=2317990, 1; Europol, iOCTA, and TRACFIN, Regulating Virtual Currencies, 2014, http://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.

platforms; and online gambling.[193] Most of these tools represent legal services and technologies that criminals can abuse because their operations exist outside of regulatory compliance and oversight. Even if some of the payments services, such as Zerocoin and Darkcoin, are known as special niche cryptocurrencies that offer total anonymity and might attract criminals,[194] they are also used for legitimate purposes and, therefore, cannot be attributed to only criminal activities.

"... [O]rganized crime groups will exploit big data 'to carry out complex and sophisticated identity frauds [at] previously unprecedented levels'."

Big Data: A Big Advantage for Criminals?

Data have always been integral to the execution of digital crime: the trade of data as a valuable illicit commodity drives the whole underground economy of cybercrime. With data becoming an asset "akin to oil in the twentieth century"[195] for legitimate businesses, the value of this commodity has also significantly increased for criminals. The more data the industry creates and stores, the more criminals are happy to consume them.[196]

To enjoy the benefits of big data, businesses tend to aggregate vast amounts of sensitive data from various sources in one place to better analyze them.[197] Such centralization also increases the value of the data for criminals and makes companies and their databases more attractive and vulnerable to cyberattacks.[198] The trade in consumer data in the legitimate economy also makes that data more vulnerable given criminals can acquire data via legal transactions. For example, in 2013 the leading global consumer credit bureau Experian inadvertently sold sensitive data on US consumers via Court Ventures, a company it acquired in 2012, to a Vietnamese identity theft ring. Data transferred to the criminals included names, addresses, Social Security numbers, birthdays, work history, driver's license numbers, email addresses, and banking information.[199]

By exploiting the vulnerabilities of centralized data storage, criminals can develop aggressive and complex techniques to commit crimes. The acquisition of a large volume of sensitive personal data can allow for phishing schemes that target individuals rather than businesses or certain demographic groups and, therefore, are harder to detect.[200] Moreover, Europol predicts that in the future organized crime groups will exploit big data "to carry out complex and sophisticated identity frauds [at] previously unprecedented levels."[201] Highly personalized scams can target a particular person on the basis of details from a social networking profile or from financial activity. Further development of biometrics in combination with big data might enable criminals to create false identities that could be used both digitally and in the real world.[202] All of these risks have to be taken into account when developing technical and legal responses to both offline and online crime.

193 Filipkowski, "Cyber Laundering." See also Council of Europe, The Use of Online Gambling for Money Laundering and the Financing of Terrorism Purposes, 2013, http://www.coe.int/t/dghl/monitoring/moneyval/activities/MONEYVAL(2013)9_Onlinegambling.pdf and Ingo Fiedler, Online Gambling as a Game Changer to Money Laundering? Institute of Commercial Law, University of Hamburg, April 30, 2013, http://ssrn.com/abstract=2261266.

194 TRACFIN, Regulating Virtual Currencies; see also Europol, iOCTA.

195 Raymond D. Moss, "Civil Rights Enforcement in the Era of Big Data: Algorithmic Discrimination and the Computer Fraud and Abuse Act," March 9, 2016, Columbia Human Rights Law Review 48.1, 2016: 1.

196 Marc Goodman, Future Crimes (New York: Knopf Doubleday Publishing Group, 2015), 137.

197 Colin Tankard, "Big Data Security," Network Security 2012, no. 7 (July 2012): 5–6.

198 Jose Gutierrez, Thomas Anzelde, and Galliane Gobenceaux, Risk and Reward: The Effect of Big Data on Financial Services, Leading Trends in Information Technology, Stanford University, Summer 2014, https://web.stanford.edu/class/msande238/projects/2014/BigDataFinance.pdf, 18; Lidong Wang and Cheryl Ann Alexander, "Big Data in Distributed Analytics, Cybersecurity, Cyber Warfare, and Digital Forensics," Digital Technologies 1, no. 1 (2015): 22-27, doi: 10.12691/dt-1-1-5, and Tankard, "Big Data Security," 5-6.

199 Brian Krebs, Experian Sold Consumer Data to ID Theft Service, Krebs on Security, October 20, 2013, https://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/.

200 Trend Micro, Addressing Big Data Security Challenges: The Right Tools for Smart Protection, 2012, http://www.trendmicro.de/media/wp/addressing-big-data-security-challenges-whitepaper-en.pdf, 4.

201 Europol, Exploring Tomorrow's Organized Crime, 2015.

202 Ibid.

Illegal Profits and Big Data: New Challenges, New Opportunities?

Prevention, Detection, and Disruption of Illicit Financial Flows

The banking industry and law enforcement agencies employ various tools to investigate crime and comply with regulations, such as the Know Your Customer requirement.[203] These tools range from anti-money-laundering software for financial industries to special equipment for digital crime investigations and electronic evidence collection.

Every year, software vendors offer industry and law enforcement agencies cutting-edge technical solutions for fighting financial crime. Some of them, like Egmont Secure Web and FIU.net, are specifically tailored to tackle the problem of illicit financial flows by managing requests for financial intelligence sharing from abroad and providing secure information exchange for this purpose.[204] Technology is employed to analyze data from beneficial ownership databases—databases that collect information about companies' owners and organizational structures and link them together—and to obtain electronic records about transaction trails to detect corruption and tax evasion by connecting seemingly unrelated transactions and activities.[205]

However, due to the increasing volume of data flows, neither law enforcement nor private companies can continue to monitor suspicious behavior using traditional tools based only on linear data.[206] Therefore, big data analytics, which can process and analyze nonlinear datasets and link together seemingly disconnected data, is considered a powerful "weapon of choice."[207] Big data tools have been revolutionary[208] in replacing or complementing manual techniques, connecting previously disconnected dots, and enabling quick responses to threats—all of which makes it easier to react before malicious activity has caused significant damage.[209] Big data analytics is able to predict security breaches by identifying abnormalities and quickly processing large amounts of linear and nonlinear data from different sources.[210] Moreover, big data solutions can not only stop criminal acts, they also play a significant role in predicting them before they occur, thus facilitating new, proactive approaches to fighting illicit financial flows.[211]

Big data analytics is also addressing the cross-border elements of illegal financial flows. Analytics makes data sharing between law enforcement agencies faster and more efficient and helps transnational crime investigations by identifying patterns.[212] Big data tools also help with mapping and visualization[213] to provide a broader picture of the illicit financial flows and identify affected geographical areas, industry players, channels, and suspects.[214]

The benefits of using big data to tackle crime and illicit money transfers have become obvious in recent years. Old investigation tools cannot analyze the ever-growing amounts of unstructured data. Thus, big data tools have been implemented in different areas and used by governments, private industry,

203 Know Your Customer is a process implemented by banks to obtain information about their customers' identities to ensure that the banking system is not misused. In many countries, anti-money laundering regulations require that banks implement this process.

204 TRACFIN, Annual Analysis and Activity Report 2013, http://www.economie.gouv.fr/files/ra_tracfin_anglais_2013.pdf.

205 Tatiana Tropina, Do Digital Technologies Facilitate Illicit Financial Flows, World Bank, 2016, http://documents.worldbank.org/curated/en/896341468190180202/pdf/102953-WP-Box394845B-PUBLIC-WDR16-BP-Do-Digital-Technologies-Facilitate-Illicit-Financial-Flows-Tropina.pdf.

206 Heather Adams, Fighting Financial Crime with Data, Accenture, 2015, https://www.accenture.com/t20160519T222110w/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_6/Accenture-Fighting-Financial-Crime-with-Data.pdf, 4.

207 Deloitte, Insight on Financial Crime: Challenges Facing Financial Institutions, 2014, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-insight_on_financial_crime.pdf, 5.

208 Europol, Exploring Tomorrow's Organized Crime, 2015, 43.

209 Executive Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, United States Government, 2016, https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf; Joe Goldberg, "Tackling Unknown Threats," Network Security 12, 2014: 16-17.

210 Digital Reasoning, Unstructured Data: A Big Deal in Big Data, http://www.digitalreasoning.com/resources/Holistic-Analytics.pdf, 2. See also Wang and Alexander, "Big Data in Distributed Analytics."

211 Deloitte, Insight on Financial Crime: Challenges Facing Financial Institutions, 2014, http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-insight_on_financial_crime.pdf; Trend Micro, Addressing Big Data Security Challenges, 5; Wang and Alexander, "Big Data in Distributed Analytics"; and Jill Coster van Voorhout, Tesse Alleblas, and Ting Zhang, Curbing Illicit Financial Flows: The Post-2015 Agenda and International Human Rights Law, The Hague, November 2015, http://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/11/PB8-Illicit-Financial-Flows.pdf, 10.

212 Houses of Parliament, Big Data, Crime, and Security, POSTnote, no. 470 (July 2014), researchbriefings.files.parliament.uk/documents/POST-PN-470/POST-PN-470.pdf, 3.

213 One example of such an infographic can be found at Dawson and Li, *Top 20 Countries Losing Money from Illicit Financial Flows*, Thomson Reuters Foundation, 2013, http://news.trust.org//item/20131211124740-udist/.

214 Van Voorhout, Alleblas, and Zhang, Curbing Illicit Financial Flows, 10. See also Shaun Hipgrave, "Smarter Fraud Investigations with Big Data Analytics," Network Security 12, 2013: 8.

nongovernmental organizations, and journalists to detect and investigate illegal transactions.

How Is Big Data Being Used to Tackle Illicit Financial Flows?

Financial Industry

In the age of digital crime, holistic approaches to crime detection have also been embraced by the financial industry, which suffers from increasing vulnerability to fraud and is a vehicle for money laundering. While facing significant financial losses from fraudulent activities, the financial industry also bears the largest burden of regulatory compliance. In most countries, banking regulations require financial intermediaries to share information with regulators and law enforcement about suspicious transactions even if the illegality of the act has not been proven.[215]

Myriad bank transactions happen every day. Traditional systems that are based on the analysis of structured data, such as credit card transactions, and on small samples of data cannot tackle the problem of detecting complex illegal schemes.[216] But, big data analytics can use structured and unstructured raw data from different sources, such as geolocation data and those from mobile devices and social media, to detect fraudulent activities, unearth hidden connections between accounts, and track the relationship between the sources and beneficiary.[217] As a result, big data analytics is replacing traditional approaches that rely on "red flag" alerts and linear data analysis with predictive models based on processing large volumes of data, such as transactions history and payment activity patterns, in real time.[218]

Likewise, regulators are also using big data analytics to carry out predictive analysis of money laundering in the financial industry. Big data analytics are being used by financial institutions to review successful investigations, identify indications of money laundering, and develop automated rules and universal templates for the industry to better fight the practice. Furthermore, big data tools are helping collect more detailed information from the industry and analyze it in more advanced ways.[219]

Big data analytics are also helping detect the misuse of new types of payments, especially virtual currencies based on blockchain technology. Despite the great degree of anonymity blockchain offers, big data tools can make it possible to track and match information on certain types of transactions, making sure that actions are legitimate and genuine. Given the recent calls to consider options for regulating blockchain,[220] big data analytics could be employed not only so regulators and enforcement agencies can detect illicit financial flows via blockchain, but also to encourage the voluntary creation of more secure and trusted digital currencies and payment systems in cases when no effective regulatory frameworks are found.

Trade-Based Money Laundering

Similarly, big data tools help detect trade-based money laundering, which includes over- and under-invoicing, multiple invoicing, over- and under-shipment, and other techniques that allow criminals to move funds across borders in the form of goods. The use of automated text analytics combined with web-analysis and web-crawling is considered to be a revolutionary development to ensure transparency in global trade.[221]

Governments and the private sector use big data algorithms to analyze both structured and unstructured transactions data. When combined with multiple records from different countries and institutions, big data can uncover suspicious patterns such as mismatches in corresponding documentation, shipment routes, and details; discrepancies between goods descriptions and shipment documents; multiple deposits; and other

215 Stavros Gadinis and Colby Mangels, "Collaborative Gatekeepers," Wash. & Lee L. Rev. 73, no. 2 (2016), http://scholarlycommons.law.wlu.edu/wlulr/vol73/iss2/6, 802.

216 Gutierrez, Anzelde, and Gobenceaux, Risk and Reward, 10; IBM, Combat Credit Card Fraud with Big Data, 2013, http://www.intel.de/content/dam/www/public/us/en/documents/white-papers/combat-credit-card-fraud-with-big-data-whitepaper.pdf, 2.

217 Bashyam Selvaraj, Combating Fraud and Money Laundering: How the Financial Services Industry Can Leverage Big Data, Tata Consulting Services, 2015, http://www.tcs.com/SiteCollectionDocuments/White-Papers/Combating-Fraud-Money-Laundering-0415-1.pdf, 1-3; Intel, Reduce Money Laundering Risks with Rapid, Predictive Insights, Solution Brief, 2015, http://www.intel.de/content/dam/www/public/emea/xe/en/documents/financial-services/final-aml-solution-brief.pdf, 2.

218 Selvaraj, Combating Fraud and Money Laundering, 3. See also Helena Forest, Evelyn Foo, Donya Rose, and Dmitriy Berenzon, Big Data: How It Can Become a Differentiator, Deutsche Bank, 2015, http://cib.db.com/insights-and-initiatives/flow/35187.htm, 12; Hipgrave, "Smarter Fraud Investigations," 8, and Daniel Mayo, Assessing the Role of Big Data in Tackling Financial Crime and Compliance Management, OVUM, 2016, http://www.oracle.com/us/industries/financial-services/fs-big-data-fccm-wp-2861557.pdf, 8.

219 Such tools have been employed in the United States by FINSEC. See Holly Gilbert, *Treasury Department Using Advanced Analytics to Help Detect, Prevent Money-Laundering,* 2013, http://www.predictiveanalyticsworld.com/patimes/treasury-department-using-advanced-analytics-to-help-detect-prevent-money-laundering/1043/.

220 As mentioned earlier in this paper, FinCEN in the United States and FATF have called for monitoring the regulatory issues and possibly creating regulatory frameworks for digital currencies.

221 John A. Cassara and Chip Poncy, Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement, Wiley, 2015, 164.

issues.[222] Since the trade finance business relies on paper documents related to specific transactions, big data analytics, especially text analytics, can effectively tackle trade-based money laundering.[223]

Box 4.3. Big Data to Tackle Trade-Based Money Laundering in Developing Countries

In November 2016, DC-based nonprofit Global Financial Integrity launched a new database tool—FTrade—that is geared toward helping developing countries. It can analyze prices in real time and measure trade misinvoicing risks for eighty thousand goods categories.[224]

Terrorist Financing

Tracking terrorist financing is yet another area where big data analytics can be useful. Some of the national and international efforts in this field have already been based on using large volumes of data to track terrorist money. For example, under the European Union-US Terrorist Finance Tracking Program, data on international bank transfers are passed, under the management of Europol, to the US Treasury for further assessment.[225] Recently, Danish journalists were able to establish links between terrorism financing and value-added-tax (VAT) refund scams by using big data analytics instruments: different datasets collected from public records were scraped and compiled to identify critical nodes and patterns, which were further verified by journalists.[226] The analysis resulted in a documentary, which was broadcast in Denmark, and sparked the launch of a further investigation by the Danish Security and Intelligence Service.[227]

In the United States, FinCEN uses advanced analytics tools to detect terrorist financing. The data gathered by FinCEN—via special rules that help identify transactions by particular terrorist organizations—generate matches in advanced data analytics systems for review and exploration. The results are passed to law enforcement and the intelligence community for further investigation.[228] Furthermore, in 2016 FinCEN proposed a rule that would require crowdfunding portals to enact policies and procedures to prevent money laundering and terrorist financing.[229] This rule would extend the application of big data analytics to include monitoring crowdfunding for signs that it is being used to finance terrorism.

Tax Crimes

Governments and international organizations are currently trying to determine how big data can best tackle offshore tax evasion. Successful examples already exist in this field. For instance, the United Kingdom's tax and customs authority has been effectively using big data analytics to tackle the problem of tax fraud. Likewise, the Internal Revenue Service (IRS) in the United States is using big data analytics—quantitative algorithms and statistical models—to detect fraud and taxpayer identity theft.[230] Additionally, the OECD has developed special programs to tackle tax avoidance and base erosion and profit shifting.

Box 4.4. Big Data to Fight Tax Fraud: A United Kingdom Case Study

The United Kingdom's tax and customs authority (Her Majesty's Revenue & Customs, or HMRC) employs the big data tool Connect to detect tax evasion and tax fraud. Connect makes it possible to bring together and analyze billions of pieces of HMRC internal data. It performs searches of information, which would otherwise be difficult to find, to elicit patterns and connections that uncover crime. HMRC reported that between April 2013 and April 2014 it was able to recover £2.6 billion by using this technology, with an initial investment of £45 million (including five years of running costs).[231]

222 PwC, Goods Gone Bad: Addressing Money-Laundering Risk in the Trade Finance System, January 2015, http://www.pwc.com/us/en/risk-assurance-services/publications/assets/pwc-trade-finance-aml.pdf.

223 Ibid., 13.

224 Global Financial Integrity, "GFI Launches Database—GFTrade—to Help Developing Countries Generate Millions in Additional Public Revenue," November 9, 2016, http://www.gfintegrity.org/press-release/gfi-launches-database-gftrade-to-help-developing-countries-generate-millions-in-additional-public-revenue/.

225 Statewatch, Note on Big Data, Crime, and Security: Civil Liberties, Data Protection, and Privacy Concerns, April 3, 2014, http://www.statewatch.org/analyses/no-242-big-data.pdf, 2.

226 EurActive, Big Data Revolutionizes Europe's Fight against Terrorism, 2016, https://www.euractiv.com/section/digital/news/big-data-revolutionises-europes-fight-against-terrorism/; see also Global Editors Network, "The VAT Hustlers," 2016, http://community.globaleditorsnetwork.org/content/vat-hustlers-0.

227 The Local DK, "Terror Suspects Tied to VAT Scam in Denmark," January 25, 2016, http://www.thelocal.dk/20160125/terror-suspects-tied-to-financial-fraud-in-denmark.

228 FinCEN, *Statement of Jennifer Shasky Calvery*.

229 C. Todd Gibson, Michael McGrath, and Ken Juster, *FinCEN Proposal to Impose AML Obligations on US Funding Portals,* K&L Gates, 2016, https://www.fintechlawblog.com/2016/05/fincen-proposal-to-impose-aml-obligations-on-u-s-funding-portals.

230 Charles S. Clark, "IRS and SEC Detect Fraud Patterns in Heaps of Data," Government Executive, October 16, 2012, http://www.govexec.com/technology/2012/10/irs-and-sec-detect-fraud-patterns-heaps-data/58816/.

231 United Kingdom Houses of Parliament, "Big Data, Crime, and Security," Postnote, July 2014, 3.

Big data analytics can help law enforcement agencies with criminal investigations, allowing them to deal with large amounts of data to identify connections between seemingly unrelated pieces of information. *Photo credit:* Reuters/Jonathan Ernst.

Law Enforcement: Crime Prevention and Crime Control

Big data tools equip law enforcement agencies with the powerful analytical processes that improve both proactive and reactive approaches to policing. Such tools are helpful not only in online crime investigations, where law enforcement has to deal with the growing amount of data that need to be analyzed, but also in investigating any complex situations, like organized crime, where it is necessary to identify connections between seemingly unrelated pieces of information. Big data analytics can be used to store, combine, and match all existing information, categorize content, and establish correlations. Furthermore, big data tools are used to identify risks, understand crime patterns, and share information between agencies.[232]

Big Data and Big Challenges

While the promise of big data analytics has not yet been fully delivered, big data tools are being used successfully. Nevertheless, both governments and the private sector must consider many factors before fully enjoying the benefits that big data tools bring to the prevention, detection, and investigation of crime and illegal money transfers.

Big Data and Human Capacity

While able to bring significant improvements to tackling illicit financial flows, big data tools alone are not the answer; they are just a part of the

232 Justin Heinze, "Fighting Crime with Data: How Law Enforcement Is Leveraging Big Data Analytics to Keep Us Safe," Better Buys, 2014, https://www.betterbuys.com/bi/fighting-crime-with-data/; "How Big Data Analytics Can Be the Difference for Law Enforcement," SAS, https://www.sas.com/en_us/insights/articles/risk-fraud/big-data-analytics-for-law-enforcement.html; Abdullahi Muhammed, "A Look into Big Data Applications for Law Enforcement," Smart Data Collective, 2016, http://www.smartdatacollective.com/oxygenmat/382813/look-big-data-applications-law-enforcement.

response.[233] Even the most sophisticated technical solutions require humans to use the results and determine future actions.[234] While big data tools enable people to perform analyses that can identify illegal financial flows, they also rely on people to ask better questions, see the broader picture, establish links, find correlations, and, ultimately, make decisions.[235]

The human factor is especially important given the danger of wrong and misleading data and the possibility of incorrectly interpreting data. It is critical to ensure the quality, authenticity, and integrity of data for big data analytics, but mistakes can occur due to human error.[236] Therefore, law enforcement agencies[237] and private industry[238] must work on capacity building and developing specialized knowledge in advanced data analytics to better ensure that the data being analyzed are sound and that the analysts can interpret results correctly.

Box 4.5. Bitcoin and Money Laundering

In January 2016, the Dutch police arrested ten people in conjunction with an international investigation into a money laundering scheme that used a cryptocurrency—bitcoin—to launder up to twenty million euros from online drug deals. Some of the suspects were operating as bitcoin traders who had acquired the currency through the illegal trade in drugs; others were involved in exchanging the cryptocurrencies for euros to withdraw them from ATMs (automated teller machines). The alarm that led to the investigation and subsequent arrests was raised by the banks, because eventually the criminals combined the use of cryptocurrencies with traditional banking and used their bank accounts to deposit large sums of money to then quickly withdraw from ATMs.[239]

Big Data Privacy Concerns and Safeguards

The principal challenges for big data solutions are the following: 1) addressing concerns about the vulnerability of databases containing personal data[240] and 2) ensuring the legality, necessity, and proportionality of analyzing data to tackle criminal activity.[241] Privacy issues are very important for the industry given the increased use of big data analytics to prevent malicious activity. Some industry players have already recognized ethical and privacy risks. According to Deutsche Bank, "one bank removed face recognition algorithms from its set of analytics, because it did not even want to be seen as being able to use it."[242] Nevertheless, there is an ongoing debate about how industry can help alleviate these challenges.

In the age of big data, addressing privacy concerns and maintaining appropriate security safeguards are also of the utmost importance for law enforcement and intelligence agencies. Data processing for the purposes of crime prevention and criminal investigation in many countries is subject to strict safeguards, checks, and balances. For this reason, law enforcement must be cautious when implementing big data solutions to avoid overstepping legal boundaries.

Big Data Tools and Capacity Building in Developing Countries

Illicit financial flows have devastating effects on developing countries. While big data analytics can help tackle the problem more effectively, the lack of regulatory and enforcement instruments in place to control financial crime and tax evasion will not be fixed by technical solutions. Therefore, in addition to technical tools, developing countries need to institute coherent policies, regulatory frameworks, and human capacity building. One of the biggest challenges is ensuring big data solutions can tackle all vulnerabilities in financial systems that enable illicit financial flows in developing countries.

233 Trendmicro, *Addressing Big Data Security Challenges: The Right Tools for Smart Protection*, White Paper, 2012, http://www.trendmicro.de/media/wp/addressing-big-data-security-challenges-whitepaper-en.pdf; Surfwatch, Big Data, Big Mess, 2.

234 Articol Bănărescu, "Detecting and Preventing Fraud with Data Analytics," Emerging Markets, Queries in Finance and Business, Procedia Economics and Finance 32, 2015: 1832–1833.

235 Conrad Constantine, "Big Data: An Information Security Context," Network Security, January 2014, 19. See also Surfwatch, Big Data, Big Mess, 3.

236 Forest, Foo, Rose, and Berenzon, Big Data, 20.

237 Europol, Exploring Tomorrow's Organized Crime, 43.

238 Forest, Foo, Rose, and Berenzon, Big Data, 21.

239 "Ten Arrested in Netherlands over Bitcoin Money-Laundering Allegation," *Guardian*, January 20, 2016, https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy; Daniel Dob, "Dutch Police Arrests 10 Men for Bitcoin Money Laundering," The Merkle, January 20, 2016, http://themerkle.com/dutch-police-arrests-10-men-for-bitcoin-money-laundering/; and Organized Crime and Corruption Reporting Project, "10 Arrested in Netherlands in Bitcoin Operation," January 22, 2016, https://www.occrp.org/en/daily/4841-10-arrested-in-netherlands-in-bitcoin-operation.

240 Wang and Alexander, "Big Data in Distributed Analytics"; Neil Richards and Jonathan King, "Three Paradoxes of Big Data," 66 Stanford Law Review Online 41, September 3, 2013; Forest, Foo, Rose, and Berenzon, Big Data; and Statewatch, "Note on Big Data."

241 Houses of Parliament, Big Data, Crime and Security, 1.

242 Forest, Foo, Rose, and Berenzon, Big Data, 21.

"Follow the Money": The Nexus of Digital Technologies and the Law

Big data tools could potentially bridge the technology gap between law enforcement agencies and sophisticated criminals. However, big data solutions do not come in a vacuum. Big data tools may solve technical problems by tracing, reporting, and predicting crime, but there are complex legal problems associated with tackling illegal money that existed long before digital technologies enabled new illicit financial flows.

Digital criminal activities can easily bypass national legal frameworks and borders that national regulators and law enforcement agencies cannot. National regulators and law enforcement agencies can enforce only the laws of the country in which they operate and they can do so only within their own national borders; therefore, they must rely on mutual legal assistance to stop criminal activities. In other words, though technological solutions, even those as promising as big data analytics, can provide powerful crime-fighting equipment, they do not fix—or bridge—all legal gaps. As a result, it will be impossible to fully harness big data's ability to fight crime and money laundering without concurrently facilitating cross-border data flows, investigations, and the exchange of electronic evidence; harmonizing regulatory and legal frameworks; and developing procedural tools and common digital forensics standards.

Lastly, the existence of thousands of stakeholders in the digital economy calls for public-private cooperation between industry and governmental bodies. While regulated intermediaries, such as entities in the financial industry, can certainly employ big data or other technological tools to better comply with anti-money laundering regulations or to protect themselves from financial fraud, there are thousands of unregulated payment providers and other intermediaries outside the scope of compliance procedures that lack incentives to contribute to the effort of mitigating illicit financial flows. Thus, it is important to find those incentives and promote collaborative voluntary approaches. Good solutions should be multi-faceted and include proper national legal frameworks; mutual legal assistance instruments able to cope with the speed of information transfers; frameworks for self-regulation, public-private cooperation, and raising awareness; and a commitment to the ongoing education of users about how to avoid crimes like identity theft.

Recommendations

- Governments, law enforcement, and private industry should employ big data analytical tools to tackle illicit financial flows; these tools have significant potential to develop solutions that would complement all previously isolated efforts to fight financial crime.
- Since big data analytics requires people to analyze results and determine appropriate actions, governments and private industry should recognize that one of the keys to success is building the human capacity to best use these innovative tools.
- Using big data tools requires governments and industry to address privacy considerations; safeguarding people's privacy should be an integral part of using big data analytics.
- Big data analytics requires proper legal frameworks that address trans-border criminal investigations, mutual legal/regulatory assistance, and compliance at the national level. To enjoy the benefits of big data, governments must implement proper laws and regulations surrounding its use and be ready to update them in the face of unforeseen technological challenges.
- Given that both governments and industry face the same technical, privacy, and ethical challenges in implementing big data tools for tracing illicit financial flows, there should be an ongoing dialogue and partnership between government and industry to build trust, share information, and develop industry standards.
- Using existing and new big data tools should be considered part of an ongoing process and long-term comprehensive strategy to tackle the problem of illicit financial flows. This multi-faceted strategy should comprise both reactive and proactive approaches and include technical and legal tools, public-private cooperation, and future risks analysis.

Conclusion

No single technical or legal solution, or any combination, will completely solve the problem of illicit financial flows. Illicit profit flows and crime will possibly exist as long as humanity does. However, big data analytics, when implemented correctly, can be a game changer for tackling financial crime and money laundering: technology can empower law enforcement agencies with the tools that enable them to both react to complex crime and money laundering and predict it. Nevertheless, to fully benefit from big data solutions, tools need to be complemented by proper legal frameworks, human capacity building, and working mechanisms to support cross-border crime investigations. Ultimately, any technology, no matter how revolutionary it could be, should be considered one part of a long-term strategy to tackle crime and abuse of the financial system—a strategy that should not only be able to address the current risks, but anticipate future ones.

CHAPTER 5

Big Data: Mitigating Financial Crime Risk

Miren B. Aparicio

Miren B. Aparicio
Counsel and Senior Consultant, The World Bank Global Practice

Financial crime legislation seeks to enhance transparency in financial transactions and restrict or prevent criminals from using banks and other non-financial sector entities to launder money. Financial integrity laws help prevent money laundering, terrorist financing, bribery, and corruption.[243] Big data is used to comply with regulatory obligations and fight financial crime.

The effectiveness in fighting financial crime is often hindered by the quality and quantity of available data and by financial integrity regulatory asymmetry across jurisdictional boundaries. There are also tensions between the principles that stand behind the rights of transparency and security in financial integrity laws versus data privacy in international data flows.

On the one hand, financial crime legislation requires banks[244] to collect information about who is and who controls any customer (Know Your Customer, or KYC, obligations), employee, or vendor at the beginning of a legal relationship and on an ongoing basis. There are even recordkeeping obligations after the relationship has ended. To fulfill their regulatory requirements, banks need to obtain and analyze comprehensive and quality data from their customers and screen them against sanctions lists provided by authorities, for each country in which the bank operates.

On the other hand, data privacy laws could hinder banks' ability to use big data to fight financial crime. Data privacy laws threaten global banks' ability to adhere to their duty to know their clients and beneficial owners when operating across borders if they make it more difficult for banks to

243 Anti-money laundering (AML), counter-terrorist financing (CTF), and anti-bribery and anti-corruption laws (ABAC) will be jointly referred to as "financial integrity laws" or "financial crime laws", with main focus on "AML laws" in this chapter.

244 The term "banks" will be used broadly in this chapter and include financial services firms, such as banks, brokers, or dealers in securities; mutual funds; and futures commission merchants and introducing brokers in commodities.

acquire this information or impede international data flows.[245] Data privacy rules are nevertheless important. Anytime an organization collects customer data, it must ensure that it complies with privacy rules, and preserves private data from cyberattacks.

Global data, which are essential to fighting crime and terrorism, cannot be processed without technology. Data analytics tools augment the ability to analyze data, which was previously structured by automated systems. However, technological tools are only as good as the underlying data they analyze, which is why accurate and quality data are essential. Mining big data is a critical component of an effective anti-money laundering program, and involves extracting and analyzing data that are both structured and unstructured and that reside both in-house and externally. As a result, for analytics tools to effectively mitigate financial crime risks, privacy laws should include exemptions for transparency and security purposes, which should be agreed upon at a global level.

This chapter analyzes the international transparency standards by the Financial Action Task Force (FATF) and the Basel Committee of Banking Supervision. It also analyzes the trends in financial crime laws in the United States and the European Union (commonly considered reference legislation), as well as the regulatory gaps that might be exploited by "bad actors." It then examines the data analytics tools used by the financial sector, its supervisors, and governments to process big data and fight financial crime. Finally, it explores technology innovation (fintech/regtech, smart contracts, and distributed ledgers technologies), and new opportunities for collaboration between the private and public sectors to manage evolving threats.

What Laws and Regulations Are in Place to Help Mitigate Risks?

Criminal activities know no boundaries, so it is important to look beyond the jurisdictional competences of supervisors and law enforcement authorities and promote international cooperation. To make it more difficult for criminals to integrate funds into the financial system, banks are required by national laws to analyze and process data from clients and their transactions that move money across borders. The occasional gaps, which are exploited by criminals, arise from the regulatory asymmetry in the implementation of the FATF 2012 recommendations, and their lack of enforcement at a global level.

International Guidelines

The Financial Action Task Force is the international anti-money laundering (AML) standard-setting body, which was established in response to mounting concern over money laundering by the G7 at the Paris summit in 1989.[246] Hosted by the Organisation for Economic Co-operation and Development (OECD), FATF issued its first round of recommendations in 1990. The recommendations are not bulletproof: Not all FATF members (currently thirty-five countries and two international organizations) criminalize money-laundering offenses or specify which crimes can serve as predicates for money laundering prosecutions. Moreover, the recommendations do not have the force of law.[247] However, they have become the world's blueprint for effective national and international controls for combating money laundering and terrorism financing, even more after the events of September 11, 2001.[248]

The Basel Committee on Banking Supervision, established in 1974 by central bank governors, promotes sound supervisory standards worldwide. In 1988, the Basel Committee set up principles for effective banking supervision and identified deficiencies in a large number of countries.[249] Even among countries with well-developed financial markets, the extent to which banks follow Know Your Customer rules and employ effective client due diligence practices varies, as noted in the 2001 reference paper *Customer Due Diligence for Banks*.[250] Banks are expected to identify their customers, monitor their accounts to identify transactions that do not conform to normal activity for that customer, investigate red flags, and report suspicious transactions of money laundering to competent authorities. Additional guidelines since 1988, including the "Sound management of risks related to money laundering and financing of terrorism" in 2016, address the need for global banks to adopt a global approach in fighting financial crime, applying a sound KYC program, and employing an automated transaction monitoring

245 See Customer Due Diligence in section Tools to Mitigate Risk.

246 "What We Do," FATF, http://www.fatf-gafi.org/about/, accessed January 9, 2017.

247 Financial Action Task Force (FATF), *The Forty Recommendations and Interpretative Notes*, 2012, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

248 FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, 2012, updated 2016, 7-9.

249 Basel Committee on Banking Supervision, *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering,* 1988, http://www.bis.org/publ/bcbsc137.pdf.

250 Know Your Customer (KYC) is the term employed by banks to refer to Customer Due Diligence processes. Basel Committee on Banking Supervision, *Customer Due Diligence for Banks*, October 2001, http://www.bis.org/publ/bcbs85.pdf.

system (data analytics tools)[251] to both the parent bank (or head office) and all of its branches and subsidiaries worldwide.[252] This proposal by the Basel Committee for banks of supervising clients' activities at a global level employing data analytics tools is a sound risk management goal to prevent financial crime. However, as the Institute of International Finance points out in a recent study, data privacy laws challenge banks' ability to fulfill this goal and FATF should work to improve the effectiveness of its member states' information sharing regimes.[253]

Anti-Money Laundering (AML) Reference Laws

Recent Trends in EU AML Directives

The first European Union (EU) AML Directive of 1991 was confined to drug trafficking, as defined in the 1988 Vienna Convention.[254] The fourth AML Directive (4AMLD) was adopted in 2015 and needs to be transposed into AML national laws by June 2017. This directive introduces an explicit requirement for companies to maintain adequate, accurate, and current information on their beneficial ownership records.[255] This information must be made readily available to competent authorities, designated entities, and any member of the public who can demonstrate a legitimate interest, upon request. EU member states need to create a central beneficial owners' registry and show that they have taken appropriate steps to identify, assess, understand, and mitigate AML/Counter Terrorist Financing (CTF) risk, including with respect to beneficial ownership information. This will also be achieved by way of a National Risk Assessment to be conducted by each EU member state.

After the Paris terrorist attacks in 2015, the European Commission presented (on February 2, 2016) an action plan to strengthen the fight against terrorist financing.[256] The action plan focuses on two main strands of action: tracing illicit financial flows and preventing terrorists from moving funds or other assets; and disrupting the sources of revenue used by terrorist organizations by targeting their capacity to raise funds.

"After the Paris terrorist attacks in 2015, the European Commission presented an action plan to strengthen the fight against terrorist financing."

The action plan listed a number of concrete measures that were immediately put into practice by the European Commission and laid out a path forward to review existing legislation and propose new legislation. As part of the action plan, the European Commission adopted a proposal to amend the 4AMLD (also referred to as "5AMLD" due to the substantial character of the proposed amendments) in July 2016. The revised directive addresses five tasks: (1) ensuring a high level of safeguards for financial flows from high-risk non-EU countries; (2) enhancing the powers of the EU Financial Intelligence Units (FIUs) and facilitating their cooperation; (3) centralizing national bank and payment account registers or central data retrieval systems in all member states; (4) tackling risks linked to anonymous prepaid instruments (e.g., prepaid cards); and (5) addressing terrorist financing risks linked to virtual currencies.

The European Commission proposed expanding the scope of the revised 4AMLD to include virtual currency exchange platforms and custodian wallet providers. FIUs would be able to have direct access to any information held by any obliged entity (even when the reporting entity has not filed a Suspicious Transaction Report). In addition, EU member states will now be obliged to set up a central registry or mechanism to identify the owners of bank and payment accounts on an automatic basis and FIUs will have direct access to these national registers.

Furthermore, the European Commission's proposal creates a harmonized and enhanced approach across the EU for performing due diligence on high-

251 Basel Committee on Banking Supervision, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, 2016, 6-16.

252 See also, "General Guidelines on Account Opening and Customer Identification," Basel Committee on Banking Supervision, February 2013, http://www.bis.org/publ/bcbs85annex.htm and Basel Committee on Banking Supervision, *Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, February 2016, http://www.bis.org/bcbs/publ/d353.pdf.

253 Institute of International Finance, Deploying Regtech Against Financial Crime, March 2017, https://www.iif.com/publication/research-note/deploying-regtech-against-financial-crime

254 The EU directives harmonize national AML standards and need to be transposed into laws by EU member states; even if they are not transposed, they have a direct effect. See "The Direct Effect of European Law," Eur-Lex, January 14, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14547.

255 Eur-Lex, *Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing*, May 20, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476157559137&uri=CELEX:32015L0849, accessed January 9, 2017.

256 European Commission, *Anti-Money Laundering and Counter Terrorist Financing: Stronger Rules to Respond to New Threats*, 2016, http://ec.europa.eu/justice/criminal/document/files/aml-factsheet_en.pdf.

risk non-EU countries. This harmonized list of actions will set minimum requirements to be applied by all EU member states and will encompass a number of checks, including on customers, the purpose and nature of the business relationship, and the source of funds.

The Council of the European Union adopted its negotiating position on December 19, 2016, and the Parliament followed with its position on February 28, 2017.[257] The final text is likely to be agreed to in 2017 by the Council and Parliament, though both institutions have different objectives, with the Parliament focusing on transparency and tax evasion and the Council on terrorist financing.[258]

Finally, the European Commission proposed a package to measure the EU's capacity to fight the financing of terrorism and organized crime, delivering on the commitments made in the action plan against terrorist financing from February 2016. The package includes a proposed directive that would establish the criminalization of money laundering for all member states (with the exception of Denmark and Ireland), a proposed regulation that would implement tighter controls on large cash flows, and a proposed regulation to strengthen the mutual recognition of criminal asset freezing and confiscation orders within the European Union.

Recent Trends in US AML Laws

Enacted in 1970, the Bank Secrecy Act (BSA) is the primary US anti-money laundering regulatory statute. It was followed by the world's first anti-money laundering law, the Money Laundering Control Act of 1986.[259] Motivated by the attacks of September 11, 2001, it was amended by the USA Patriot Act.[260]

In particular, the USA Patriot Act of 2001 AML rules have extraterritorial reach and are especially relevant for correspondent banking relationships. Under Section 311, the Treasury Department has the authority to apply special measures to address primary money laundering concerns related to specific banks in foreign jurisdictions.[261] For instance, in 2005, the Treasury designated Banco Delta Asia in Macau as a "primary money laundering concern" and served the bank with a 311 order because it had facilitated a range of illegal activities for North Korea, including counterfeiting $100 bills and money laundering.[262] Practically overnight, banks throughout the region stopped doing business with the Banco Delta. A ripple effect around the international banking community led to the freezing, scrutiny, and isolation of North Korea from the banking system. This result was remarkable for several reasons: the United States could not have proposed any trade sanctions, since there was no trade with North Korea at the time; Banco Delta did not have US accounts to be frozen; and North Korea was not the subject of any United Nations (UN) measure or sanction.[263] Another recent example is Russia, which would like to see an easing of US sanctions on Western financing for its banks and oil companies, because fewer sanctions could easily boost growth by a percentage point or more by some estimates.[264]

The US Treasury can compel US banks to apply gradual protective measures, from recordkeeping practices to closing correspondent accounts. US banks have to apply special due diligence measures and respond to questions about any client or foreign bank they deal with, including who its owners are and the nature of its regulatory oversight.[265] For any correspondent banking account managed by a US financial institution, the US Treasury can request any

257 EU Council, *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC,* December 19, 2016, http://data.consilium.europa.eu/doc/document/ST-15605-2016-INIT/en/pdf.

258 EU Parliament, *Report on the Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, March 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN

259 Federal Financial Institutions Examinations Council, *Money Laundering Control Act of 1986*, http://www.ffiec.gov/bsa_aml_infobase/documents/regulations/ml_control_1986.pdf.

260 US Department of Justice, *The USA Patriot Act: Preserving Life and Liberty*, 2001, https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

261 "Special Measures: Overview," *Bank Secrecy Act Anti-Money Laundering Examination Manual*, Section 311 of the USA Patriot Act (2001), which amends the Bank Secrecy Act (1970), https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_031.htm.

262 Bryan Borrough, "In 'Treasury's War,' Missiles for a Financial Battlefield," *New York Times*, August 31, 2013, http://www.nytimes.com/2013/09/01/business/in-treasurys-war-missiles-for-a-financial-battlefield.html.

263 Samuel Rubenfeld, "Q&A: Juan Zarate, the author of 'Treasury's War,'" *Wall Street Journal,* September 26, 2013, http://blogs.wsj.com/riskandcompliance/2013/09/26/qa-juan-zarate-author-of-treasurys-war.

264 Neil Buckley, "Buoyant Putin Still Needs Washington to Cut a Deal on Sanctions," *Financial Times*, December 19, 2016, https://www.ft.com/content/13cbbdca-c76b-11e6-9043-7e34c07b46ef. See also Max Seldom and Courtney Weaver, "Trump to Call Putin as He Considers Lifting Russia Sanctions," *Financial Times*, January 27, 2017, https://www.ft.com/content/581eff4e-e49b-11e6-8405-9e5580d6e5fb.

265 US Department of Justice, *The USA Patriot Act*, Section 312, http://ithandbook.ffiec.gov/media/resources/3356/con-usa_patriot_act_section_312.pdf.

A woman holds bank notes at Banco Delta Asia in Macau, China. *Photo credit:* Reuters/Paul Yeung.

records regarding the account, even those located outside of the United States, including the identity of each beneficial owner of the foreign bank, unless the bank is publicly traded.[266]

Requirements for banks to know their corporate clients' beneficial owners are also increasing in the United States.[267] The USA Patriot Act had already contemplated requiring beneficial ownership information as part of customer due diligence obligations, but the act did not provide a definition of a beneficial owner, so the identification requirements were unclear.

However, the Bank Secrecy Act passed in May 2016, which will become effective in 2018, will address this issue for companies when a new account is opened.[268] Trusts, on the other hand, do not have beneficial ownership identification requirements under the new legislation.[269] This is a significant gap.

266 US Department of Justice, *The USA Patriot Act*, Section 319(b) and implementing regulations, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_027.htm.

267 The final rule (§ 1010.230) released by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) on May 6, 2016, to obtain and record beneficial ownership information will increase the customer due diligence obligations of covered financial institutions, which will have two years to implement the new requirements on beneficial ownership, as part of their obligations under the Bank Secrecy Act in Title 31.

268 The beneficial ownership definition includes any individual who owns directly or indirectly 25 percent or more of the equity interests of the corporate customer. See Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, 31 CFR Parts 1010, 1020, 1023, et al., https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

269 Ibid. Covered financial institutions include federal regulated banks and credit unions, mutual funds, brokers and dealers in securities, futures comissions merchants and introducing brokers in commodities.

What Are the Regulatory Gaps?

There is a lack of consistent AML regulations across the global community. The different playing fields of controls internationally, caused by deficient AML laws and often by their lack of enforcement by national authorities, create opportunities for "bad actors" to operate in many jurisdictions; this should be tackled as a global priority. Emerging countries, as recently recommended by the Financial Stability Board (FSB), need stricter bank supervision.[270]

Currently, FATF members (thirty-five countries) do not fully implement the FATF 2012 recommendations, and many countries do not implement them at all. This regulatory asymmetry creates jurisdictional gaps, which are exploited by bad actors. The exclusion of politically exposed persons (PEPs), beneficial owners, and "gatekeepers" of the financial sector (such as lawyers, real estate professionals, and trusts) from transparency requirements is a regulatory gap that threatens the global community, as revealed by the Panama Papers.[271] Virtual currencies and other new businesses can be used by bad actors to move money globally.

Financial Sector Gatekeepers

The FATF recommendations contain AML guidelines for the financial sector's "gatekeepers," including trusts and company services providers, lawyers, real estate professionals, casinos, dealers in precious metals and stones, those in the life insurance sector, and money services businesses.[272] Many of these businesses remain unregulated internationally, with AML laws addressing only the financial sector. Some examples of vulnerabilities are as follows:

Law Firms. The FATF 2016 December report on the United States has called law firms' pooled accounts a vulnerability.[273] Tens of billions of dollars every year move through opaque bank accounts managed by law firms that create a gap in US money-laundering defenses. US law firms protect the confidentiality of their pooled accounts citing attorney-client privilege.

Real Estate. In 2016, the US Treasury's Financial Crimes Enforcement Network (FinCEN) issued several Geographic Targeting Orders (GOTs),[274] which apply to title companies located in six major metropolitan areas in the United States (New York, Miami, Los Angeles County, San Diego County, the San Francisco area, and the county that includes San Antonio, Texas) and require them to identify the beneficial owners of legal entities, partnerships, or representatives that make all-cash purchases of high-end residential real estate. GOTs[275] are valid for 180 days and were renewed on February 24, 2017, for a similar period. FinCEN[276] found that about 30 percent of the transactions were related to a beneficial owner with a previous suspicious activity report. The information obtained confirmed the use of shell companies to launder money through the purchase of luxury real estate in "all-cash" transactions and led to enforcement actions. For instance, in June 2016, the Department of Justice seized more than $1 billion in assets from the 1Malaysia Development Berhad fund. The sovereign wealth fund's embezzled assets were transferred into the United States using shell companies and the client bank accounts of law firms to buy luxury real estate properties in Los Angeles, New York, and London.[277]

Trusts and Bearer Shares Corporations. The Panama Papers leak in 2016 also revealed a serious need to supervise non-financial sector entities (such as trust services companies and law firms), despite previous country assessments by FATF. Two years prior, in June 2014, FATF identified strategic deficiencies in Panama, which expedited the adoption of an AML legislation package. Panama's vulnerability to money laundering was that not all financial and non-financial sectors were subjected to AML regulations and supervision. This was addressed in the new legislation and provided the justification, after some technical assistance, to remove Panama

270 Caroline Binham, "Stricter Bank Supervision Needed in Developing Nations, Say Policymakers," *Financial Times*, December 19, 2016, https://www.ft.com/content/13cbbdca-c76b-11e6-9043-7e34c07b46ef.

271 "The Panama Papers: A Torrential Leak," *Economist*, April 9, 2016,http://www.economist.com/news/international/21696497-huge-trove-documents-has-revealed-secrets-offshore-business-presaging-tougher.

272 FATF, *Risk-Based Approach Guidance for Legal Professionals*, October 23, 2008, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/riskbasedapproachguidanceforlegalprofessionals.html

273 Rachel Louise Ensign and Serena Ng, "Money Laundering Loophole: Law Firms," *Wall Street Journal*, December 27, 2016, A1 and A6.

274 US Department of Treasury, "Treasury Announces Key Regulations and Legislation to Counter Money Laundering and Corruption, Combat Tax Evasion," Press Release, May 5, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx.

275 US Department of Treasury, *Geographic Targeting Order*, February 21, 2017, https://www.fincen.gov/sites/default/files/shared/Real%20Estate%20GTO%20February%202017%20-%20Generic.pdf.

276 US Department of the Treasury, "FinCEN Renews Real Estate 'Geographic Targeting Orders' to Identify High-End Cash Buyers in Six Major Metropolitan Areas," Press Release, February 23, 2017, https://www.fincen.gov/news/news-releases/fincen-renews-real-estate-geographic-targeting-orders-identify-high-end-cash.

277 Louise Story, "US to Expand Tracking of Home Purchases by Shell Companies," New York Times, July 27, 2016, http://www.nytimes.com/2016/07/28/us/us-expands-program-to-track-secret-buyers-of-luxury-real-estate.html?_r=0.

from the FATF (grey) list of countries with strategic deficiencies in February 2016.[278] However, the leak of the law firm Mossack Fonseca shortly after (in April 2016) revealed the continued lack of transparency and extended use of shell companies to launder money and evade trade sanctions.[279] It also suggested that FATF international surveillance of AML country frameworks should be strengthened through independent reviews.

A recent US State Department report points to the country's serious AML deficiencies:

> Numerous factors hinder the fight against money laundering, including the existence of bearer share corporations, a lack of collaboration among government agencies, lack of experience with money laundering investigations and prosecutions, inconsistent enforcement of laws and regulations, and a weak judicial system susceptible to corruption and favoritism. Money is laundered via bulk cash and trade by exploiting vulnerabilities at the airport, using commercial cover and free trade zones (FTZs), and exploiting the lack of regulatory monitoring in many sectors of the economy. The protection of client secrecy is often stronger than authorities' ability to pierce the corporate veil to pursue an investigation.[280]

Fintech: Crowdfunding, Online Lending Platforms, P2P Lending

Online lending platforms, peer-to-peer (P2P) lending, and equity crowdfunding—the raising of capital by selling unregistered securities to investors or lenders over the Internet—are rapidly growing industries in the United States, United Kingdom (UK), and China, according to Morgan Stanley.[281] However, Standard and Poor's has raised concerns about the online lending platforms' capacity to comply with key financial regulatory principles and the quality of the data that the platforms keep and on which they base their loan underwriting decisions.

The 2015 FATF report on Emerging Terrorist Financing Risks points to crowdfunding as an alternative way to transfer funds abroad for terrorism finance purposes, citing the FIU of Canada, which has reported several instances "where individuals under investigation for terrorism-related offences, have used crowdfunding websites prior to leaving and/or attempting to leave Canada."[282] Several cases link P2P lending or crowdfunding platforms with terrorism financing. Online lending platforms should screen lenders and investors against designated terrorist and sanctioned entity lists, take steps to detect fake investors, and report suspicious transactions. The questionable due diligence practices of some crowdfunding platforms internationally, combined with regulatory fragmentation, make crowdfunding vulnerable to exploitation by criminals.

In the San Bernardino, California, terrorist attack, in which a married couple killed fourteen people and wounded others, one of the shooters obtained a loan from a peer-to-peer lending site to finance the attack.[283] The problem in this case was not the source of funding (which was legitimate), but the clients' identification and end use of Syed Raheel Farook's loan, which was not to consolidate loans, as he had alleged, but to purchase guns and munition. P2P lending risk lies in the anonymity of these loans, compared with traditional bank loans to a person who has an account with the bank and whose financial activities can be monitored.

Another potential threat is to cybersecurity and identity theft. In October 2015, US telecommunications giant T-Mobile reported a data breach that affected fifteen million customers. The stolen data could be used to create fake lender or investor profiles to launder money. As an example, fake investors (with stolen T-Mobile identities) could crowdfund a sham company that purports to do charitable work abroad. The investors could transfer funds to the company by purchasing (worthless) equity, and the company could transfer the money abroad under the guise of its business.

278 The Inter-American Development Bank drafted the new AML legislation, and provided technical assistance to Panama to be removed from the FATF grey list "Panamá prepara nueva ley contra el blanqueo de capitals," La Estrella De Panamá, August 12, 2014, http://laestrella.com.pa/economia/panama-prepara-nueva-contra-blanqueo-capitales/23795230.

279 "The Lesson of the Panama Papers," *The Economist*, April 9, 2016, http://www.economist.com/news/leaders/21696532-more-should-be-done-make-offshore-tax-havens-less-murky-lesson-panama-papers.

280 US Department of State, *International Narcotics Control Strategy Report, Vol. II*, 2016, http://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/index.htm.

281 By 2020, Morgan Stanley forecasts online lenders will reach $47 billion, or 16 percent of total US small and medium enterprise (SME) approvals, Smittipon Srethapramote et al., *Global Marketplace Lending: Disruptive Innovation in Financials*, Morgan Stanley, May 19, 2015, http://bebeez.it/wp-content/blogs.dir/5825/files/2015/06/GlobalMarketplaceLending.pdf.

282 FATF, *Emerging Terrorist Financing Risks*, "Case Study 19: Crowdfunding," October 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf, 31-32.

283 Darrell Delamaide, "Loan to Terror Couple Challenges Regulators," *USA Today*, December 15, 2015, http://www.usatoday.com/story/money/2015/12/15/shooting-terrorism-online-loans-san-bernardino/77358520/; "FBI Will Investigate San Bernardino Shootings as Terrorist Act," Federal Bureau of Investigation, December 4, 2015, https://www.fbi.gov/news/stories/fbi-will-investigate-san-bernardino-shootings-as-terrorist-act.

Since 2013, in the United States, crowdfunding platforms have been subject to AML requirements.[284] Under Securities and Exchange Commission and Financial Industry Regulatory Authority (FINRA) rules, equity crowdfunding AML programs must comply with Bank Secrecy Act obligations analogous to those applicable to a broker-dealer, including establishing and maintaining effective customer identification on investors; conducting background checks on each officer, director, and holder of 20 percent voting power of the issuer; monitoring and reporting suspicious activity and complying with requests for information from FinCEN and denying access to its services if it believes the issuer or the offering presents a potential for fraud.

Online lending businesses should employ automated tools to detect and prevent AML risks.[285] Similar to online banking, platforms should use compliance intelligence tools to prevent crowdfunding project initiators from secretly raising funds for illicit purposes. A December 2016 Harvard Business School white paper proposed automating the regulatory compliance activities for online lending platforms and creating a concrete regulatory action plan, including a limited national charter.[286]

On December 2, 2016, the Office of the Comptroller of the Currency (OCC) proposed issuing special purpose national bank charters for financial technology (fintech) companies.[287] In March 2017, the OCC issued a licensing manual draft supplement or Fintech Charter[288] for comments. The OCC will consider applications for special purpose national bank licenses from financial technology companies, which operate one of the core banking activities of "paying checks" (broadly referred to as payment systems) or lending money (including any new form of leasing or discounting). The Fintech Charter would require governance and a risk assessment, including AML, among other regulatory requirements and would subject the firms to OCC supervision. Overall, it would make it possible for fintech companies to provide services across the United States.

Fintech companies would be able to voluntarily apply for a national charter and benefit from uniform (federal) regulation and supervision by the OCC. Chartered fintech companies would need to adopt AML risk-mitigation programs and automated tools similar to banks. As the OCC notes, discounting notes, purchasing bank-permissible debt securities, engaging in lease-financing transactions, and making loans are forms of lending money. Similarly, issuing debit cards or engaging in other means of facilitating payments electronically are the modern equivalent of paying checks. The OCC would consider on a case-by-case basis the permissibility of new activities.

Some EU countries, such as the UK and Spain, have specifically regulated crowdfunding, but it is not regulated at the European level—though some other countries consider crowdfunding as an activity covered under the Markets in Financial Instruments Directive.[289] Regarding lending-based crowdfunding, the European Banking Authority recommends that online platforms should, at a minimum, require borrower background checks; have strong AML policies and procedures in place; offer transparent information regarding their directors, stakeholders, and beneficial owners; and have enough technical capacity and expertise to maximize online security.[290]

The World Bank InfoDev study[291] projects that the market value of crowdfunding will be $96 billion by 2025. It also recommends crowdfunding should occur only on portals that are registered with a national regulatory body that oversees securities, or through clearing houses that conduct mandatory background checks for issuers and investors and require auditing and financial disclosures. Very few crowdfunding platforms meet these requirements today globally. In fact, many platforms raise

284 Equity crowdfunding is regulated by the US Jumpstart Our Business Startups Act ("JOBS Act") Title 301 ("This title may be cited as the "Capital Raising Online While Deterring Fraud and Unethical Non-Disclosure Act of 2012" or the "Crowdfund Act"); Crowdfunding, 78 Fed. Reg. 66428, 66461-65, proposed November 3, 2013, hereinafter "Regulation Crowdfunding."

285 Zachary Robock, "The Risk of Money Laundering Through Crowdfunding: A Funding Portal's Guide to Compliance and Crime Fighting," Michigan Business Entrepreneurial Law Review, Vol. 4, No. 1 (2014), http://repository.law.umich.edu/mbelr/vol4/iss1/4/.

286 Karen Gordon Mills and Brayden McCarthy, *The State of Small Business Lending: Innovation and Technology and the Implications for Regulation*, Harvard Business School Working Paper 17-042, 2016, http://www.hbs.edu/faculty/Publication Files/17-042_30393d52-3c61-41cb-a78a-ebbe3e040e55.pdf, 73 and Chapter 6.

287 Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies*, 2016, https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf.

288 Office of the Comptroller of the Currency, *Evaluating Charter Applications from Financial Technology Companies*, 2017, https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

289 Financial Conduct Authority, *A Review of the Regulatory Regime for Crowdfunding and the Promotion of Non-readily Realizable Securities by Other Media,* February 2015, https://www.fca.org.uk/publication/thematic-reviews/crowdfunding-review.pdf.

290 European Banking Authority, "EBA recommends convergence of lending-based crowdfunding regulation across the EU," February 26, 2015, https://www.eba.europa.eu/-/eba-recommends-convergence-of-lending-based-crowdfunding-regulation-across-the-eu.

291 World Bank, *Crowdfunding's Potential for the Developing World*, 2013, http://www.infodev.org/infodev-files/infodev_crowdfunding_study_0.pdf.

questions regarding the identity of issuers and investors and the fragmentation of the regulatory regimes in cross-border sourcing projects.

Remittances and Money Services Businesses

A risk-based approach should guide the regulation of remittance service providers (RSPs) and money services businesses (such as those that issue travelers checks and prepaid cards) at the global level.[292] At this time, RSPs are mostly unregulated and have different business models. However, after September 2001, the FATF Special Recommendations on Terrorist Financing provided that in order to prevent terrorist financing, informal remittance houses should be licensed and comply with risk-based AML regulatory standards that apply to banks.[293] The European Parliament acknowledges the difficulty in implementing FATF recommendations at a global level, as well as the different terminology employed across jurisdictions (also referred to as "money transfer or money service businesses" in Anglo-Saxon legal systems). The Consultative Group to Assist the Poor, housed at the World Bank, recommends a gradual implementation of AML rules that considers the level of maturity of the monetary industry in each country.[294]

RSPs receive cash from their customers that they transfer internationally through the banking system. Data on who sends and receives these payments in foreign countries are often untraceable and criminals frequently use this anonymity to their advantage. For instance, the HSBC Group paid $1.9 billion in fines to US authorities in 2012 for not supervising its RSP clients, which laundered money from drug cartels through its Mexican unit for years.[295] Mexico is the top destination for money transfers from the United States, according to estimates by the World Bank.[296] However, according to the 2009 International Monetary Fund (IMF) country report for Mexico, RSPs are not required to conduct any customer due diligence except for when transactions exceed $10,000.[297]

Since the financial crisis, remittance start-ups[298] have emerged globally using disruptive technologies such as blockchain in direct payments to mobile phones (P2P money transfers) to provide remittance services across borders. While some of them are not regulated, others are. For instance, Coins.ph is a mobile blockchain-based platform connecting over three hundred million unbanked people in Southeast Asia.[299] Blockchain helps Coins.ph facilitate remittances from any country as long as the sender is able to purchase digital currency. Coins.ph is regulated by the central bank of the Philippines (BSP) as a remittance and foreign exchange company. Since the amounts are small, KYC requirements for opening a Coins.ph account are less demanding than opening a bank account. For low-risk individuals' identification purposes, a risk-based approach permits users to take a selfie on their phone while holding a government identity document. Strategic partnerships with banks also allow Coins.ph customers to use automated teller machines (ATMs) by sending a code to their phone without the need to have a bank account or an ATM card.[300]

Virtual Currency Businesses (Exchanges and E-Wallets)

Bitcoin and other virtual currencies embody a value-transfer system that operates like a currency or a commodity, with no issuer or central authority. There are, however, inherent risks that have

292 See Committee on Payment and Settlement Systems and World Bank, *General Principles for International Remittance Services*, January 2007, http://www.bis.org/cpmi/publ/d76.pdf. "The World Bank Migration Development Brief," Issue No. 21, October 2013, 29; See also, "Let Them Remit," *The Economist*, July 20, 2013, http://www.economist.com/news/middle-east-and-africa/21581995-western-worries-about-money-laundering-are-threatening-economic-lifeline.

293 FATF, *Special Recommendations on Terrorist Financing, 2001,* reviewed 2008, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf; see also World Bank, *Guidance Report for the Implementation of the CPSS-World Bank General Principles for National Remittance Services,* Financial Infrastructure Series, 2007, http://www.worldbank.org/en/topic/paymentsystemsremittances/publication/guidance-report-for-the-implementation-of-the-cpss-wb-general-principles-for-international-remittances, 24-26.

294 European Parliament, "The Impact of Remittances in Developing Countries", p.30 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/deve/dv/remittances_study_/remittances_study_en.pdf

295 Aruna Viswanatha and Brett Wolf, "HSBC to Pay $1.2 Billion US Fine in Money Laundering Case," Reuters, December 11, 2012, http://www.reuters.com/article/us-hsbc-probe-idUSBRE8BA05M20121211.

296 Raúl Herández-Coss, *The US–Mexico Remittance Corridor: Lessons on Shifting from Informal to Formal Transfer System,* World Bank Working Paper No. 47, February 2005, http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/US-Mexico_Remittance_Corridor_WP.pdf.

297 International Monetary Fund, Mexico: Detailed Assessment Report on Anti-Money Laundering and Combating Terrorism, Country Report, 2009, 130, paragraph 146.

298 Amit, "11 Money Transfer Companies Using Blockchain Technology," Let's Talk Payments, October 23, 2015, https://letstalkpayments.com/11-money-transfer-companies-using-blockchain-technology-2/.

299 Kate, "19 Bitcoin Remittance Startups That Won't Let the Cryptocurrency Die," Let's Talk Payments, February 5, 2016, https://letstalkpayments.com/19-bitcoin-remittance-startups-that-wont-let-the-cryptocurrency-die/.

300 Chamber of Digital Commerce, Georgetown University, "Blockchain and Financial Inclusion White Paper", March 2017, p. 18-19, http://finpolicy.georgetown.edu/newsroom/news/center-releases-white-paper-blockchain-and-financial-inclusion

A chain of block erupters used for Bitcoin mining is pictured at the Plug and Play Tech Center in Sunnyvale, California October 28, 2013. A form of electronic money independent of traditional banking, Bitcoins started circulating in 2009 and have since become the most prominent of several fledgling digital currencies. *Photo credit:* Reuters/Stephen Lam.

attracted the attention of regulators. Due to the anonymity afforded by these currencies, criminals are increasingly using virtual currency exchanges and e-wallets to launder money. For instance, a high percentage of illicit financial flows from developing countries are now being transferred through trade-based money-laundering methods to avoid detection. Using virtual currencies in such international transactions makes them almost untraceable.[301]

Bitcoin's protocol, for example, does not verify participants and generates transactions that are not necessarily associated with a real-world identity. It therefore offers a level of anonymity beyond traditional credit and debit cards or online payment systems, such as PayPal. The transactions in blockchain can be tracked, but mixers can be used to hide the transactions history of any client so it becomes easier to launder money without being detected.[302] Also, the transaction records may reside with multiple entities located in different jurisdictions, which makes it difficult for law enforcement to collect information.

301 Global Financial Integrity, *Illicit Financial Flows from Developing Countries: 2004-2013,* December 2015, http://www.gfintegrity.org/wp-content/uploads/2015/12/IFF-Update_2015-Final-1.pdf.

302 FATF Report, "Virtual Currencies Key Definitions and Potential AML/CFT Risks", June 2014, p. 6 , http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed.

Criminal abuse of the bitcoin currency has already featured prominently in several high-profile laundering and fraud cases. In 2014, a board member of the nonprofit Bitcoin Foundation was charged with money laundering for allegedly conspiring with a bitcoin exchange operator to sell $1 million in bitcoins to users of the Silk Road black market.[303] That same year, Japan-based Mt. Gox, then the world's largest bitcoin exchange, announced that hackers had stolen $500 million in bitcoins from its poorly guarded system.[304] Japanese prosecutors later charged former Mt. Gox Chief Executive Officer Mark Karpeles with embezzlement, accusing him of stealing $2.66 million from clients.[305]

The emergence of virtual currency exchanges (VCEs) and other related businesses poses new risks described by the FATF 2014 paper. Anyone with an Internet connection can use them to transfer funds across borders, regardless of jurisdiction, while very few countries have issued regulations surrounding their use.[306] The IMF has pointed out that more could be done to help develop an effective international framework for the regulation of virtual currencies.[307]

In the United States, in 2013, FinCEN issued guidance and rulings on when a VCE must register as a money services business and is subject to anti-money laundering and KYC regulations. However, what constitutes an exchange can be unclear. VCEs engage in exchanging virtual currency for "real currency." However, this gets more complicated when private users (who are not regulated) offer on classified websites to sell or buy bitcoins at a premium or a discount, making the transaction anonymous. A Louisiana chiropractor exchanged more than $3 million in money orders through his credit card accounts for bitcoins that he bought on bitcoin exchanges. The reality is that unlicensed bitcoin exchanges[308] have been connected with other illegal activity.

Virtual currency exchanges, which are considered money transfer businesses in the United States, are regulated by states. While some states allow money transmitters to operate without a license, others require one. In 2015, the New York Department of Financial Services issued specific regulations for virtual currency businesses, requiring anyone conducting these activities in New York State to be licensed (Bitlicense) and to implement customer due diligence requirements and AML programs.[309]

Another challenge is supervision. There is no central oversight authority over the virtual currency exchanges or custodian wallet providers (WPs). In the United States, since 2013, VCEs and WPs have been subject to AML supervision by FinCEN at the federal level. In March 2017, the OCC issued a voluntary charter proposal for financial technology companies (Fintech Charter),[310] which would allow them to operate at the federal level under OCC's supervision.[311]

In the European Union, the 5AMLD will aim to harmonize the AML requirements among EU member states for virtual currency exchanges and custodian wallet providers and impose strict limits on prepaid cards.[312] Under the European Commission's proposal to expand the scope of the revised fourth AMLD (or 5AMLD), VCE platforms and WPs would become "obliged entities" and have to implement similar preventive measures and report suspicious transactions. The new directive would also reduce

303 Emily Flitter, "Prominent Bitcoin Entrepreneur Charged with Money Laundering," Reuters, January 27, 2014, http://www.reuters.com/article/us-usa-bitcoin-arrests-idUSBREA0Q15N20140128.

304 Yoshifumi Takemoto and Sophie Knight, "Mt. Gox Files for Bankruptcy, Hit with Lawsuit," Reuters, February 28, 2014, http://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228.

305 Taiga Uranaka, "Prosecutors File Charges against Ex-CEO of Mt. Gox Bitcoin Exchange," Reuters Canada, September 12, 2015, http://ca.reuters.com/article/technologyNews/idCAKCN0RC04620150912.

306 FATF, *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems,* June 18, 2008, http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercialwebsitesandinternetpaymentsystems.html.

307 Dong He et al., *Virtual Currencies and Beyond: Initial Considerations*, International Monetary Fund, January 2016, SDN/16/03, 36.

308 Lester Coleman, "Arrests and Prosecutions Reveal Big Vagaries in Bitcoin Selling Regulations," Cryptocoin News, May 23, 2016, https://www.cryptocoinsnews.com/arrests-and-prosecutions-reveal-big-vagaries-in-bitcoin-selling-regulations/.

309 New York State Department of Financial Services, New York Codes, Rules, and Regulations, Title 23, *Department of Financial Services,* Chapter I. *Regulations of the Superintendent of Financial Services*, Part 200. *Virtual Currencies,* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

310 US Department of Treasury, "OCC to Consider Fintech Charter Applications, Seeks Comment," Press Release, December 2, 2016, https://www.occ.treas.gov/news-issuances/news-releases/2016/nr-occ-2016-152.html.

311 Office of the Comptroller of the Currency, *Evaluating Charter Applications From Financial Technology Companies*, Comptroller's Licensing Manual Draft Supplement, March 2017, https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

312 European Commission, *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, July 5, 2016, http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf; see also Samantha Sheen, "ACAMS, 4AMLD Part 3: Virtual Currency Exchange Platforms, E-Wallet Providers and Pre-Paid Cards," Advancing Financial Crime Professionals Worldwide, July 20, 2016, http://www.acams.org/aml-resources/samantha-sheens-blog/eu-proposals-to-bolster-fight-against-financial-crime/.

the exemption regime for anonymous prepaid cards. In its proposal, the European Commission suggested deleting the exemption for prepaid cards used online, lowering the threshold for non-reloadable prepaid cards from $282 (€250) to $169 (€150), and enhancing the powers of FIUs. However, it is still unclear whether the 5AMLD would require uniform licensing or registration for VCEs and WPs, or whether each EU member state may opt for either regime. In any event, as the European Banking Authority's 2016 opinion pointed out, due to the Internet's reach, there are practical difficulties in preventing unlicensed or unregistered entities from providing digital services across borders.[313]

This problem also applies at the global level, due to the Internet's reach, since the majority of virtual currency businesses remain unregulated. The "big three" Chinese VCEs[314] issued statements in February 2017 disallowing withdrawals for a month to upgrade infrastructure and include "self-regulated" anti-money laundering controls, following regulatory pressures from the People's Bank of China. Regulation for VCEs and WPs should be addressed globally, promoting the adoption of AML, cybersecurity, and consumer protection frameworks and automating the monitoring process.[315]

Politically Exposed Persons (PEPs)

PEPs represent a high-risk category of customers for banks, and are subject to enhanced due diligence in many countries. FATF recommendations include the customer identification of both domestic and foreign PEPs. However, many AML national laws only include the obligation to identify international PEPs and often exclude domestic PEPs, which is a significant gap. The United Nations and the World Bank recommend income and asset disclosure regimes for PEPs to prevent corruption and money laundering.[316] The requirement that public officials declare their income and assets already exists in the United States for government employees, General Schedule (GS)-15 and higher.[317]

The challenge for banks in fulfilling their regulatory obligations to identify and monitor PEPs transactions is mainly that public data from official sources are difficult to obtain. Analytical software for client due diligence purposes often includes PEPs information obtained from private and (when available) public sources, media, and the Internet. However, the data contained are often difficult to analyze in cases of a potential name match, since the available information is frequently incomplete. For instance, the Central Intelligence Agency's library database of chiefs of state and cabinet members of foreign governments provides a public list of names but not dates of birth (which should be necessary for financial firms to investigate potential "false positives," i.e., name matches that do not correspond to the same person).[318] In addition, PEPs have found many ways to avoid detection, such as by opening accounts in the names of corporations, trusts, or close family members or associates.[319] The Corruption Perceptions Index published by Transparency International, a nongovernmental organization devoted to combatting corruption, ranks countries by scores.[320] Quality PEPs data should be available as part of the UN Anti-Money Laundering Information Network, which should consider establishing and maintaining a global repository of PEPs.[321] Disclosure requirements on assets before and after leaving office should be required globally as a transparency measure, following the UN's and World Bank's recommendations.[322]

313 The European Banking Authority has issued further recommendations in its 2016 opinion to adopt a more comprehensive EU regulatory regime for virtual currencies and set up a wall with the financial sector. See European Banking Authority, *Opinion of the European Banking Authority on the EU Commission's Proposal to Bring Virtual Currencies into the Scope of Directive (EU) 2015/849 (4AMLD)*, August 2016, http://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD.

314 Samburaj Das, "Bitcoin Withdrawals Postponed, to Resume after Regulatory Approval: Chinese Exchanges," Cryptocoin News, March 8, 2017, https://www.cryptocoinsnews.com/bitcoin-withdrawals-postponed-resume-regulatory-approval-chinese-exchanges/.

315 See Transaction Monitoring section. Financial Industry Regulatory Authority, *Anti-Money Laundering*, Special NASD Notice to Members 02-21, April 2002, http://www.finra.org/sites/default/files/NoticeDocument/p003704.pdf.

316 World Bank, *Public Office, Private Interests: Accountability through Income and Asset Disclosure,* 2012, https://star.worldbank.org/star/sites/star/files/Public%20Office%20Private%20Interests.pdf, 7-21.

317 The US Ethics in Government Act of 1978 sets the financial disclosure requirements for members and employees of the government. See Public Citizen, *Personal Financial Disclosure Requirements for Public Officials*, June 2011, https://www.citizen.org/documents/Personal-Financial-Disclosures-June2011.pdf.

318 CIA Library of Chiefs of State and Cabinet Members of Foreign Governements, https://www.cia.gov/library/publications/world-leaders-1/

319 World Bank, *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It,* 2011, 11-16.

320 Transparency International, "Corruption Perceptions Index 2015," 2015, http://www.transparency.org/cpi2015.

321 See United Nations International Anti-Money Laundering Information Network, "Anti-Money Laundering International Database (AMLID)," www.imolin.org/amlid/index.html.

322 World Bank, *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It,* 2011

Beneficial Owners

Transparency requirements in AML laws should go beyond the identity of corporate customers to include their controlling interests or beneficial owners; this recommendation aligns with those of FATF. In the United States, the final rule released by FinCEN on May 6, 2016, adds a new obligation for banks to obtain and record beneficial ownership information on their legal entity clients to ensure clear identification of their stakeholders and controlling interests.[323] The Bank Secrecy Act's new beneficial ownership requirements will become effective in 2018, and will create specific reporting duties with respect to each "legal entity customer" when a new account is opened. The beneficial owner is any individual who owns 25 percent of a company or significantly controls, manages, or directs a customer.[324]

The European Union's 4AMLD of 2015, which goes into effect on June 26, 2017, already follows this FATF recommendation. It sets out specific rules on the collection, storing, and access to information on the ultimate beneficial owner of companies.[325] The new definition of a beneficial owner is further specified as a natural person who ultimately has a shareholding, controlling, or ownership interest with over 25 percent of the shares or voting rights in corporate entities, land title ownership included.[326] Although there are notable differences in the positions of the Council and the European Parliament, and depending on the final agreement, the 5AMLD (or revised fourth AMLD) could widen transparency obligations by lowering the threshold below 25 percent, so that more beneficial owners would need to be identified by banks.

The 5AMLD aims to reinforce such transparency obligations by also proposing to create public access by way of compulsory disclosure of certain information on the beneficial ownership of trusts and other passive non-financial entities such as foundations. The 5AMLD needs to be adopted by the European Parliament and Council and negotiators are aiming to agree to it by summer 2017.[327] The revised fourth AMLD is scheduled to be transposed into national law by all EU member states twelve months after publication in the EU's Official Journal.

A recent example exemplifies why oversight of beneficial ownership records must be strengthened. The Financial Conduct Authority and the New York Department of Financial Services fined Deutsche Bank (DB) in 2016 for failures to pick up the beneficial owners of a Russian trading scheme used by offshore clients to launder money in London. The bank shut its investment bank in Russia as a consequence. The offsetting trades consisted of a series of mirror trades. A small broker in Russia bought from DB blue chip shares for rubles, while the same stocks were sold by a British Virgin Island holding company to DB in London for cash in dollars. An internal audit report found around two thousand similar transactions that transferred money out of Russia, bypassing AML controls and involving around $10 billion. The US Department of Justice is examining potential money laundering and sanctions evasion schemes connected to these transactions.[328] The bank has admitted that "the company has so many different technology systems that the gaps between them are open to manipulation."[329]

Tools to Mitigate Risks

The elaboration of customer risk profiles has been recently called the "fifth" pillar[330] of an AML program, due to the substantial changes introduced by the new FinCEN legislation in 2016. The other four pillars are policies, training, compliance, and independent audit functions. A strong customer due diligence program should include the following information about customers: the full identification of a customer and its beneficial owners (for legal entities), development of a "client profile" and transaction activity profiles (or transaction monitoring) in anticipation of the projected customer's activity,

323 See US Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, FinCEN Rule § 1010.230, Vol. 81, No. 91, May 11, 2016, https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions.

324 Ibid. Covered financial institutions include federal regulated banks and credit unions, mutual funds, brokers and dealers in securities, futures comissions merchants and introducing brokers in commodities.

325 Eur-Lex, *Directive (EU) 2015/849*.

326 Ibid. See definition of beneficial owner in Eur-Lex, *Directive (EU) 2015/*849, Article 3 and Articles 30 and 31.

327 *EU Parliament, Report on the Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC,* March 2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN

328 Karen Freifeld and Arno Schuetze, "Deutsche Fined $630 Million for Failures over Russian Money-Laundering," Reuters, Edition United Kingdom, January 31, 2017, http://uk.reuters.com/article/us-deutsche-mirrortrade-probe-idUKKBN15E2SP.

329 John O'Donnell, "The 'Mirror' Trades That Caught Deutsche in Russian Web," Reuters, January 31, 2017, http://www.reuters.com/article/uk-deutsche-mirrortrade-probe-scheme-idUKKBN15F23D.

330 "FinCEN's Final Rule to Enhance Customer Due Diligence Requirements for Financial Institutions," Davis Polk & Wardwell, May 31, 2016, https://www.davispolk.com/publications/fincen%E2%80%99s-final-rule-enhance-customer-due-diligence-requirements-financial-institutions/.

"Data profiling techniques can identify data quality issues; ensure standards are fulfilled; reconcile differences; and suggest solutions for identified problems. "

the investigation of unusual customer or account activity (including documentation of findings), and suspicious transaction reporting. The client profile refers to the information gathered about a customer at the account opening that is then used to analyze the customer's behavior (client monitoring) and report potential suspicious activities to the competent Financial Intelligence Unit.

Customer Due Diligence

Banks need to obtain information about potential new corporate customers before they open an account. In the case of legal entities, this includes basic information about the company's directors, shareholders, and beneficial owners. In May 2016, FinCEN issued final rules under the Bank Secrecy Act outlining new customer due diligence requirements, which involve developing customer risk profiles and abiding by Know Your Customer rules, which use customer due diligence tools to mitigate the risk of fraud.[331] Due diligence tools are, in practice, used equally by private and public sector entities. By establishing a customer risk management framework, financial institutions can effectively understand the overall risk posed by their clients. Managing customer data is key for an anti-money laundering program, even before a contractual relationship is entered into. The more a bank or a public sector agency knows about its counterparts or clients, the more likely it is that money-laundering and reputational risk abuses can be prevented.

Initially, the banks obtain KYC information from prospective customers through a series of data-gathering interviews and questionnaires before the account is opened. To determine what type of information should be obtained from clients, a group of international banks from the United States and Europe met with the Basel Institute on Governance at the Wolfsberg Group (an association of banks) in Switzerland in 1999.[332] They set up industry standards, known as the Wolfsberg AML Principles, on how to conduct client questionnaires to gather data from them and mitigate risk. These principles complement FATF recommendations with a technical approach to guide banks in customer due diligence rule implementation.[333]

Customer Profiling

Understanding the purpose of a customer relationship helps a bank formulate a risk-based approach to monitoring each customer's activities and detecting unusual behavior. To develop a customer risk profile, a bank analyzes data about the customer's annual income, net worth, domicile, and principal occupation or business, as well as the customer's history of activities with the bank.

Financial institutions continually review data that could update or enhance established customer identification information. The most common issues with customer data relate to missing or inaccurate data.[334] Not capturing comprehensive risk-relevant data that form a customer risk profile could lead to incorrectly evaluating unusual activity. The challenges can be higher in global organizations where information is not easily shared across jurisdictions or remains in silos in business units that do not communicate.[335]

Once data have been collected, the risk posed by the customer needs to be evaluated. Although the rules do not specifically require a system of risk rating, this process creates a consistent definition of risk across a business unit or an institution and eliminates subjective interpretations of risk levels in processes related to customer due diligence or in transaction monitoring. For instance, FINRA[336] has specifically required that online brokers who do not meet their clients in person should maximize the use of electronic databases to verify information about existing or prospective clients and conduct computerized surveillance on account activity to detect unusual or suspicious transactions.[337]

331 Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, 31 CFR Parts 1010, 1020, 1023, et al., May 2016, https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

332 Gemma Aiolfi and Hans-Peter Bauer, "The Wolfsberg Group," in Mark Pieth (ed.), *Collective Action: Innovative Strategies to Prevent Corruption*, (Zurich: Dike, 2012), 1-10, http://www.dike.ch/Collective_Action_Pieth.

333 Wolfsberg Group, "*Wolfsberg Principles for Correspondent Banking,* 2002, www.wolfsberg-principles.com/corresp-banking.html.

334 Issues with customer data often include missing data, multiple names in name lines, names in address lines, inconsistent data standards, duplicates, lack of additional customer information, and extract issues.

335 Rita Gemayel, "Understanding Customer Risk," ACAMS Today, September-November 2016, Vol. 15, No 4, 64-65.

336 "NASD Provides Guidance to Member Firms Concerning Anti-Money Laundering Compliance Programs Required by Federal Law," Notice to Members, FINRA, 2002, http://www.finra.org/industry/notices/02-21.

337 Ibid., 7. See FINRA's guidance to online brokers.

In general, banks use automated programs—which are usually based on a risk-scoring model and data-profiling techniques—to perform AML customer due diligence. Risk-scoring models use numeric values to create client profiles and their associated risk categories (i.e., by product, geographic area, customers who operate online only). The risk categories are then combined to give a composite score. A high-risk assessment may indicate a client needs more scrutiny or enhanced due diligence. Data quality should be addressed at system implementation to avoid creating a massive backlog. Advanced compliance systems offer sophisticated data quality solutions to analyze, cleanse, and de-duplicate customer records. Data profiling techniques can identify data quality issues; ensure standards are fulfilled; reconcile differences; and suggest solutions for identified problems. Building client profiles at the beginning of the client relationship and identifying high-risk customers can later help the bank focus its resources on monitoring transactions more accurately and effectively, based on client risk. For instance, FinCEN found that Eurobank's[338] automated system failed to adequately capture numerous transactions related to the same customer. Also, the automated system did not monitor for suspicious activity based on customer risk profiles, or the type and volume of customer transactions.[339]

Sanctions Screening

Before a bank starts doing business with a prospective customer, it must check the customer against published lists of known or suspected terrorists to mitigate the regulatory risk of dealing with sanctioned parties and comply with AML laws. This automated process is called sanctions screening and must be periodically undertaken by banks once a client relationship has been established, at least for each new transaction with a customer. The hundreds of names of individuals and businesses that appear in several lists of sanctioned parties issued by the United Nations, the US government (including the Office of Foreign Assets Control or OFAC List) need to be screened against each bank's customer databases. Global banks should be in a position to simultaneously monitor many sanctions lists issued by several countries, including notably the EU and the UK Treasury consolidated lists.[340]

Because banks cannot rely on manual controls to detect sanctioned parties from their customers' databases, good technological tools and quality structured data on each customer profile play important roles in this effort. For instance, a client name may initially match a sanctions list name (e.g., Pablo Escobar) but a check on the client's date of birth from a passport will reveal that this red flag is just a "false match" or "false positive." Banks use automated sanctions-screening tools, which aggregate all sanctioned entities and individuals. As FINRA points out, "Given the global nature of online brokerage activity, it is essential that online brokers confirm the customer data and review the OFAC List to ensure that customers are not prohibited persons or entities and are not from embargoed countries or regions."[341]

Enterprise risk solutions obtain, analyze, and process data from media, the Internet, and other private and public sources for sanctions-screening purposes. Public sources are necessary to obtain data such as birth certificates or certificates of incorporation from corporate registers. Corporate certificates of incorporation may include the names of directors, stakeholders, and other significant individuals.[342] However, public data lack uniformity across jurisdictions and are challenging for banks to collect on a global level. For instance, official identity documents vary from country to country and are nonexistent in many countries in Africa and Asia. This identity information is key to conducting sanctions-screening and customer-identification programs. In other words, access to public and private information sources is a critical component of the matching process and fundamental to reducing false positives in sanctions-screening processes. Ensuring data quality and their accessibility for AML and security purposes must be seen as a partnership between the private and public sectors, each of which is equally important.[343]

338 FinCEN, *Assessment of Civil Money Penalty*, in the matter of Eurobank, San Juan, Puerto Rico, US Department of the Treasury, 2010, https://www.fincen.gov/sites/default/files/enforcement_action/AssessmentEurobank.pdf.

339 Ibid., 4; see also Daniel Nathan and Alma Angotti, *Securities Regulation & Law Report, 44 SRLR 1410, 07/23/2012*, The Bureau of National Affairs, http://www.bna.com.

340 See Office of Foreign Assets Control, *Specially Designated Nationals and Blocked Persons List*, https://www.treasury.gov/ofac/downloads/sdnlist.pdf; United Nations, *Consolidated United Nations Sanctions List*, https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/consolidated.xsl; European External Action Service, *Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions*, https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions; UK Treasury, *Financial Sanctions: Consolidated List of Targets*, https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

341 FINRA Notice, http://www.finra.org/sites/default/files/NoticeDocument/p003704.pdf.

342 Wolfsberg Group, *Wolfsberg Statement on AML Screening, Monitoring and Searching,* 2009, http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Monitoring_Screening_Searching_Paper_(2009).pdf, 3.

343 Screening process for PEPs and sanctions requires quality data, including primary name; alias and alternate names; record

KYC Utilities

In correspondent banking relationships, a bank must rely on its foreign bank counterpart's AML controls to detect unwanted clients and process international trade finance or payment transactions on its behalf. Prior to entering into any correspondent relationships between banks, a thorough review of each counterpart's AML control framework is required by AML laws in many countries. For instance, under the USA Patriot Act, a US bank needs to apply enhanced due diligence measures to analyze the risk of doing business with each of its foreign correspondent banking counterparts.[344] In practice, this has created a glut of AML questionnaires being circulated by banks to each and all counterparts as a means of complying with due diligence requirements.

The Wolfsberg Group, an organization composed of an association of private banks, has been collaborating since 2004 with a third-party, private vendor to set up the first international "due diligence repository" for the collection and storage of data, including relevant due diligence information and documentation among member banks. Data on each financial institution at a group level (including its licenses, beneficial owners, corporate governance, directors, managers, and AML controls) are shared among financial entities upon consent, instead of exchanging standard AML questionnaires.[345]

Several providers have developed central identity management facilities or "KYC utilities" with the aim of keeping customer due diligence information in a single repository. Although it has obvious benefits for banks and customers, there is no standardized set of information that should be included in KYC utilities, since there is not a uniform definition of customer due diligence in AML laws and identification documents vary from country to country. Also, data privacy, processing, and localization rules impede the use of information in utilities, and may prevent banks from submitting relevant information to utilities. Utilities are working on solutions for these problems, but a dialogue and coordination with regulatory authorities is essential, since ultimately it could facilitate supervision.

Some KYC utilities are using distributed ledger technology, instead of a single repository, to store client due diligence information. As FINRA points on in a recent report, the responsibility ultimately cannot be transferred to the utility: "While broker-dealers may choose to outsource certain functions to a central utility or a third party on the network, firms need to be aware that they may not outsource their responsibility associated with the performance, or lack thereof, of those functions (see, e.g., "Notice to Members 05-48: Outsourcing.")[346]

SWIFT announced in January 2016 that over two thousand financial institutions in over two hundred countries and territories had signed up for their KYC utility, which maintains standardized sets of data—including KYC information for correspondent banks, fund distributors, and custodians—that can be shared among members.[347]

Supply Chain Management

Automated tools can track vendors and service providers. Due diligence tools help governments and the private sector understand how their supply chains operate and where key suppliers are located. For example, the acquisition of raw materials (e.g., conflict diamonds) can be traced: due diligence tools help provide information on country risk and gaps in transparency by fully mapping supply chains to avoid human trafficking or forced labor. These tools are used by private and public sector entities to comply with public procurement rules, sanctions, or environmental or government export controls regulations.[348] As an example, the Department of Defense and many other US agencies, which have strict procurement rules, may use automated tools similar to those used by banks to track vendors that respond to its requests for proposals.

There are many automated screening tools that analyze data related to background checks on prospective and current employees, contractors, and vendors, especially for criminal history. These are in addition to customer due diligence tools for name screening against sanctions lists and negative news. Employee background checks impede bad actors from accessing company information and systems, thereby preventing potential fraud and regulatory and reputational risks. The Federal Deposit Insurance Corporation has provided specific guidance to the financial sector, recommending a risk-focused approach (higher for managerial

type (individual, entity, vessel); gender; date of birth; age; country; address (country, city, address lines); national ID and passport number.

344 See *The USA Patriot Act*, Section 312, http://ithandbook.ffiec.gov/media/resources/3356/con-usa_patriot_act_section_312.pdf ,

345 "International Due Diligence Repository," Wolfsberg International, http://www.wolfsberg-principles.com/diligence.html.

346 FINRA, Distributed Ledger Technology: Implications of Blockchain for the Securities Industry, January 217, p. 15, http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

347 SWIFT, "SWIFT´s KYC Registry Surpasses 2,000 Financial Institutions," January 19, 2016, https://www.swift.com/insights/press-releases/swift_s-kyc-registry-surpasses-2_000-financial-institutions.

348 US Department of State, *Trafficking in Persons Report*, *Preventing Human Trafficking in Global Supply Chains*, 2015, https://www.state.gov/documents/organization/245365.pdf, 13-33.

A taxi passes a company list showing the Mossack Fonseca law firm at the Arango Orillac Building in Panama City. The International Consortium of Investigative Journalists released a database with information on more than 200,000 offshore entities that are part of the Panama Papers investigation. *Photo credit:* Reuters/Carlos Jasso.

levels) and several background screenings, including fingerprint checks against a criminal database. Some regulations prohibit any person who has been convicted of a crime involving fraud or money laundering from owning or controlling an institution or participating in managerial functions.[349]

Transaction Monitoring

The first challenge for a global bank is identifying the unusual or suspicious transactions within the massive amount of data generated by its global transactions. Big data analytics are essential for detecting illicit activities, which are hidden within layers of multibillion dollar transactions, particularly in trade-related businesses and government programs. Data analytics tools are equally applied by banks for the prevention of money laundering and by government agencies in data intensive fraud investigations.

Big data analytics aggregate data from multiple platforms and should be designed to quickly and accurately identify and flag financial transactions that involve individuals or entities included on watch lists and involved in suspicious transactions. Integrating data from multiple sources—such as linking client email and all available financial transaction data, including clients' financial records, if available—into a single big data platform would increase the accuracy of analytics.

Adopting new cognitive computing systems will increase and enhance the human capacity in the investigation and decision-making process related to clients' suspicious transactions.[350] Intelligent process

349 Federal Deposit Insurance Corporation, Pre-Employment Background Screening. Guidance on Developing an Effective Pre-Employment Background Screening Process, 2005, https://www.fdic.gov/news/news/inactivefinancial/2005/fil4605.pdf.

350 Bryan Bell and Robert A. Goldfinger, "Compliance Solutions: Combining Cognitive Computing with Human Intelligence," ACAMS Today, September-November 2016, Vol. 15, No. 4, pg. 50-51.

automation (IPA)[351] is a set of new technologies that combines robotic process automation and machine learning. IPA can replace human effort in processes that involve analyzing and aggregating data from multiple sources. As an example, IPA technologies can be programmed to monitor clients' financial activities and learn from such recognized patterns to detect unusual behavior. In doing so, data analytics tools will become more efficient in detecting patterns of suspicious transactions that may be further analyzed by compliance professionals to detect potential illicit activity.[352]

The Basel Committee's 2016 report recommends automating the monitoring process for banks that are internationally active. Effective techniques for global bank transaction monitoring should combine all client accounts. Transaction monitoring tools, whether developed internally or acquired from vendors, should scan, filter, and analyze customer account activities and data. Such automated tools "must enable the Bank to undergo trend analysis of transaction activity and to identify unusual business relationships and transactions in order to prevent [money laundering]."[353]

Since 2002, FINRA has recommended adopting computerized surveillance tools, jointly with a risk-based review and investigation of alerts, for online brokers and other global firms to detect and report suspicious transactions to law enforcement.[354] The FinCEN fines imposed on Eurobank and Wachovia suggest it would be difficult for US banks with large transaction volumes or international operations to meet FinCEN regulatory expectations for identifying and reporting suspicious transactions by relying only on manual controls. Eurobank relied mostly on manual processes to monitor transactions for suspicious activity.[355] This seemed particularly inadequate to FinCEN, given "the Bank's customer base, geographic risk and business lines, as well as the volume, scope, and types of transactions conducted at the Bank."[356]

Another challenge is setting the appropriate thresholds[357] for monitoring purposes, which often depend on the type of business account and client relationship. In transaction monitoring systems, programming is key. The adequacy of a bank's systems will be tested in an inspection visit or by an independent audit. A review of the number of unusual transactions, the way they are analyzed and documented, and finally the number and quality of suspicious activities filed with FIUs can be very revealing. A very low number of alerts compared with a high number of transactions conducted by a bank may suggest that the setting for the alert programming is wrong, particularly if the business involves high-risk jurisdictions, transactions, or customers. Also, a sound suspicious activity–monitoring program for global banks needs to include all client accounts and transactions across business lines and multiple countries.[358] For instance, in the Wachovia case, FinCEN found that "Wachovia's automated transaction monitoring systems were inadequate to support the volume, scope, and nature of international money transfer transactions conducted by the Bank. . . . The number of alerts or events generated by the Bank's automated transaction systems was capped to accommodate the number of available compliance personnel."[359]

Independent Audits

Compliance reviews and internal audits are independent functions that oversee business units and are the second and third lines of defense of an AML program. As FinCEN in the Wachovia fine noted, there was room for improvement in the independent validation of the audit function as a tool to mitigate risk: "In addition, the monitoring system's programming, methodology, and effectiveness were not independently validated to ensure that the models were detecting potentially suspicious activity."[360]

The volume of regulatory requirements and data involved renders manual compliance inadequate for analyzing customer profiles and account transactions. Data are meaningless unless they are organized in a way that enables people to analyze

351 Albert Bollard, Elixabete Larrea, Alex Singla, and Rohit Sood, *The Next-Generation Operating Model for the Digital World*, McKinsey & Company, 2017, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-next-generation-operating-model-for-the-digital-world.

352 George Anadiotis, "Big Data versus Money Laundering: Machine Learning, Applications and Regulation in Finance," ZDNet, http://www.zdnet.com/article/big-data-versus-money-laundering-machine-learning-applications-and-regulation-in-finance/.

353 Basel Committee on Banking Supervision, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, 6.

354 Financial Industry Regulatory Authority, *Anti-Money Laundering*, Special NASD Notice to Members 02-21.

355 FinCEN, *Assessment of Civil Money Penalty*, in the matter of Eurobank, San Juan, Puerto Rico.

356 Ibid.

357 Nathan and Angotti, "Broker-Dealer AML Transaction Monitoring: The Devil's in the Details."

358 Ibid.

359 US Department of the Treasury, Financial Crimes Enforcement Network, *Assessment of Civil Money Penalty*, in the matter of Wachovia Bank, No. 2010-1, https://www.fincen.gov/sites/default/files/enforcement_action/100316095447.pdf, 4.

360 Ibid., 4.

them and make decisions based on the results of those analyses. An independent audit can test the sophistication of data analytics tools, as well as their thresholds and the potential biases in algorithms.[361] The employment of data analytics tools and the quality and frequency of audits to validate such risk management systems can be revealing about the institution and its management's commitment to fighting financial crime. Banks have to employ qualified and experienced audit and compliance staff empowered to investigate suspicious transactions and make independent decisions. In addition, high-quality, independent, and frequent external audits are needed to test controls.

Training Programs

Many AML laws around the world require banks to implement mandatory training programs for their employees as a preventive measure. For instance, the USA Patriot Act requires AML programs to include an ongoing employee training program.[362] A sound training program for global banks should include a practical course focused on how to avoid money laundering and sanctions risks within the parameters of an employee's regular job routine. Its content should include applicable legal requirements and references to policies and procedures but also other fundamental aspects, such as how to recognize vulnerabilities and make the right judgements by showing real examples of good and bad control tests; how suspicious transactions activity is recorded and documented; when and how to raise concerns or seek support from financial crime compliance and risk professionals; and a broader and deeper understanding of the financial crime risks within a business context. Such AML programs need to be risk-based and function-specific—business lines must be able to identify and report suspicious transactions for the AML program to be effective.

Additional Tools to Help Governments and Law Enforcement Manage Evolving Threats

Regtech

Regtech (derived from the words regulation and technology) is often used to explain how technology can help banks and regulators fulfill their regulatory compliance reporting obligations and supervisory duties.[363] Regtech uses digital technologies (including big data analytics, cloud computing, and machine learning) to automate compliance and risk-management processes, facilitate regulatory reporting, and track regulatory changes worldwide. As an example, regtech makes it possible to identify the "one to many" relationship for the first time (i.e., where one control satisfies many regulations, or where a single regulation requires multiple controls). Different forms of technological innovation can facilitate the automation of data reporting from regulatory filings of suspicious transactions (SARs) or currency transaction reports.[364] In particular, they can set up intelligent queries and algorithms to detect SARs. It may also be easier for financial institutions to maintain records for regulators, audits, or inspection visits.[365]

Big data analytics and data science also have wide applications for the private sector and governments to enhance financial crime supervision, particularly in areas such as trade-based money laundering. Data mining, network analysis, and algorithms designed to assess probabilistic measures of suspicious activity in financial transaction data can help with compliance by mining the data related to clients' activities and uncover hidden patterns in the flow of the funds. This could help increase transparency in transactions related to the multibillion dollar global trade and finance industry as well as those in the shadow banking industry, which challenge law enforcement authorities. Both types of transactions are highly fragmented, global, interconnected, and governed by multiple regulators.[366]

Regtech solutions have promising applications to streamline compliance costs and processes.

361 Kevin Petrasic, Benjamin Saul, James Greig, and Matthew Bornfreund, "Algorithms and Bias: What Lenders Need to Know," White & Case, January 20, 2017, https://www.whitecase.com/publications/insight/algorithms-and-bias-what-lenders-need-know.

362 See *The USA Patriot Act*, Section 352.

363 Fintech Circle Innovate CEO Nicole Anderson coined the term "regtech." See "The FinTech Influencers: FinTech, RegTech, and the Disruption of Banking's Services," Herrington Starr, May 26, 2015, http://www.harringtonstarr.com/fintech-influencers-fintech-regtech-disruption-bankings-services.

364 Institute of International Finance, *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*, March 2016, p. 4, https://www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting.

365 European Securities and Markets Authority, European Banking Authority, and European Insurance and Occupational Pensions Authority, *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions*, JC 2016 86, Joint Committee of the European Supervisory Authorities, December 2016, file:///Users/mirenapariciobijuesca/Downloads/jc-2016-86_discussion_paper_big_data.pdf, 27.

366 Caitlin Long, "*Why Financial Regulators Are Warming to Blockchains and Rightfully So*" in Alt-M Ideas for an Alternative Monetary Future, (April 2016), http://www.alt-m.org/2016/04/26/why-financial-regulators-are-warming-to-blockchains-and-rightfully-so/

Artificial intelligence systems and robotic processes automation have huge potential to complement big data analytics, such as for anti-money laundering and client identification, which are related to compiling and checking data on customers and transactions. A number of regtech providers are developing systems for using blockchain for digital identity purposes.

"Several countries are testing the development of a digital identity. . . When approved, it could be leveraged by banks to facilitate KYC processes."

An example of a new information source to conduct KYC and background checks are web crawlers, which can scan the Internet and deliver their data to big data infrastructures in real time.[367] In the future, machine learning could be promising to monitor suspicious transactions on a risk-based customer profile.

Regtech technologies, such as biometric validation for digital identity and KYC purposes—including facial, voice, fingerprint, and iris recognition—are evolving rapidly. Citigroup's 2017 *Digital Disruption Revisited*[368] report explores regtech as an opportunity for banks to explore the use of artificial intelligence and biometric identification for anti-money laundering and client identification, since "over the longer term, a nationwide [know your customer] utility could be beneficial to the whole society, and many regulators and governments are working towards this ideal."[369]

Customer due diligence infrastructure requires analyzing information from private and public sources in different languages and formats, which vary from country to country. Regtech providers can aggregate data worldwide. As an example, identity verification companies provide access to data collected in fifty countries from a variety of sources; data intelligence platforms collect information about financial crimes from media sources.

Regtech innovation can also help governments provide citizens with a digital identity.[370] As the US Department of Commerce's *Digital Identity Guidelines* define it:

> Digital Identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject. In other words, accessing a digital service may not mean that the physical representation of the underlying subject is known. Identity proofing establishes that a subject is actually who they claim to be. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity.[371]

Several countries are testing the development of a digital identity, such as the Monetary Authority of Singapore, which is developing a digital proof of identity tool on mobile phones. When approved, it could be leveraged by banks to facilitate KYC processes. Estonia[372] is another example of progress in this area. Estonians have a digital identity embedded in a SIM card, which they can use for digital signatures for every legal document and voting.[373]

Another successful example is Aadhaar, a digital identity program that has been introduced in India and is targeting one billion citizens on a voluntary basis, to be identified and authenticated by the use of biometrics (fingerprints and scan of the iris).[374] The Aadhaar digital identity project aims

367 Institute of International Finance, Deploying Regtech Against Financial Crime, March 2017 p 17 ss. https://www.iif.com/system/files/32370132_aml_final_id.pdf

368 "What FinTech VC Investments Tell Us about a Changing Industry," Citi GPS, January 23, 2017, https://www.privatebank.citibank.com/home/fresh-insight/citi-gps-digital-disruption-revisited.html.

369 Martin Arnold, "Banks' AI Plans Threaten Thousands of Jobs," *Financial Times*, January 25, 2017, https://www.ft.com/content/3da058a0-e268-11e8-8405-9e5580d6e5fb.

370 See the Draft Digital Identity Guidelines, provided by National Institute of Standards and Technology, DRAFT NIST Special Publication 800-63-3 *Digital Identity Guidelines*, US Department of Commerce, 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html.

371 Ibid.

372 See "Fact," e-Estonia.com, https://e-estonia.com/facts/.

373 Citigroup Global Perspectives and Solutions, *Digital Disruption – Revisited – What FinTech VC Investments Tell Us about a Changing Industry*, January 2017, https://ir.citi.com/rc3XP%2FtfuLrOmpDrBN2nNfJpkI7892Pd71h7%2BpDMbIosIS3u8kcgSiJoKWuI6p6RLpMUB0DYajQ%3D, 40.

374 Reserve Bank of India, *Committee on Comprehensive Financial Services for Small Businesses and Low Income Households*, 2013, via World Bank, http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1339624653091/8703882-1339624678024/8703850-1368556147234/India-Financial-Inclusion-Report-RBI-CMTE-CFS070114EFL.pdf, 7-21. See also World Bank, Transforming Digital Identity in India, http://www.worldbank.org/en/news/video/2016/01/13/transforming-government-digital-identity-in-india

to avoid fraud with the creation of a centralized database including information on citizens deterred by any government agency. Digital identity can promote financial inclusion. Any potential welfare and healthcare benefits provided by the Indian government can be disbursed through a digital account associated with each citizen's mobile phone using this system.[375]

Digital identity uses are promising but also present the technical challenge of cybersecurity: "…because this process often involves the proofing of individuals over an open network, and always involves the authentication of individual subjects over an open network to access digital government services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks."[376]

Blockchain, Distributed Ledger Technologies, and Smart Contracts

Financial supervisory agencies are welcoming blockchain as a transparent ledger that will help supervise securities trading and settlements due to the "practical impossibility of a single national regulator collecting sufficient quality data . . . to recreate a real-time ledger of the highly complex, global swaps trading portfolios of all market participants."[377] Digital Asset Holdings' December 2016 *Digital Asset Platform: Non-Technical White Paper* defines a distributed ledger technology (DLT) as "a record of transactions or other data which exists across multiple distinct entities in a network."[378] Its application for different uses is evolving rapidly, from transaction registries to other forms of data and encoded business logic. Central banks, exchanges, governments, and financial market participants are starting to use DLTs for several purposes, including issuing digital currencies and creating securities infrastructure with reduced operational risk, data integrity, and increased market transparency while protecting confidentiality.[379]

Smart contracts were defined by computer scientist Nick Szabo in 1996 as a "set of promises, specified in digital form, including protocols within which the parties perform on these promises."[380] The white paper prepared in December 2016 by the Smart Contracts Alliance, an initiative of the Chamber of Digital Commerce, explores in detail twelve use cases for businesses. Smart contracts are typically deployed on a blockchain, although they can be used on other platforms. Blockchain technology uses encryption messages, which are bundled together in a software-generated container (a block), relating to a particular smart contract. In permissioned (closed) blockchains, an administrator incorporates the encrypted messages into the secured data. The white paper points to promising potential applications of smart contracts for digital identities, company registrations, financial data or land title recordings, supply chains, insurance, mortgages, trade finance, and clinical trials, among other areas.[381]

Smart contract applications for digital identities (for individuals and companies) could represent a valid alternative for mitigating financial crime risk and streamlining compliance with KYC processes for financial firms. A digital identity for individuals and legal entities could potentially be issued by a regulatory agency that controls the identity's personal data and is able to securely disclose them to different counterparties (such as banks) in a blockchain, as needed.[382] An interesting and innovative public initiative by Delaware (the Delaware initiative), in partnership with a fintech company,

375 World Bank, *Digital Identity Toolkit: A Guide for Stakeholders in Africa,* June 2014, http://documents.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf.

376 National Institute of Standards and Technology, DRAFT NIST Special Publication 800-63-3 *Digital Identity Guidelines*, US Department of Commerce, 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html.

377 Commodity Futures Trading Commission Commissioner J. Christopher Giancarlo speech before the CATO Institute, "Cryptocurrency: The Policy Challenges of a Decentralized Revolution," April 2016, US Commodity Futures Trading Commission, http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-14; see also Mary Jo White, "Opening Remarks at the SEC Fintech Forum" US Securities and Exchange Commission, November 2016, https://www.sec.gov/news/statement/white-opening-remarks-fintech-forum.html.

378 Digital Asset Holdings, *The Digital Asset Platform,* December 2016, http://hub.digitalasset.com/hubfs/Documents/Digital%20Asset%20Platform%20-%20Non-technical%20White%20Paper.pdf?utm_campaign=whitepaper-non-tech&utm_medium=email&_hsenc=p2ANqtz-9kX1tI0v3HDSL4FBF2JCelw-TrrhFvbkqsrl_lqGfRwSbWk00bu1VqUmQqgK_SSKdlxDAtq05ciM8q-BsommkSxGP3EF-UgkJAhInC9DE4eQx89hI&_hsmi=38825746&utm_content=38825746&utm_source=hs_email&hsCtaTracking=fc1f9260-0c14-472a-967e-c9cb3095f953%7Cba8116ac-3c0b-43f3-a880-d60c4bc1d707, 4.

379 Ibid., 27.

380 See Nick Szabo, "Foreword" in *Smart Contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, December 2016, https://gallery.mailchimp.com/a87f67248663abe55ad9325d6/files/Smart_Contracts_12_Use_Cases_for_Business_Beyond.pdf?utm_source=Chamber+of+Digital+Commerce&utm_campaign=4123b7a006-EMAIL_CAMPAIGN_2016_12_06&utm_medium=email&utm_term=0_e6622a916a-4123b7a006-338085917

381 *Smart Contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, December 2016, https://gallery.mailchimp.com/a87f67248663abe55ad9325d6/files/Smart_Contracts_12_Use_Cases_for_Business_Beyond.pdf?utm_source=Chamber+of+Digital+Commerce&utm_campaign=4123b7a006-EMAIL_CAMPAIGN_2016_12_06&utm_medium=email&utm_term=0_e6622a916a-4123b7a006-338085917.

382 See also Ibid., 6-48.

A bitcoin ATM machine enables the user to convert cash to bitcoins via a QR code transfer to an application on their mobile device. *Photo credit:* Reuters/Mike Blake.

is the development of a new public repository to incorporate companies in 2017—corporations will have the choice of registering either via traditional stock certificates or on a blockchain. Registering companies through blockchain could facilitate performing due diligence, registering beneficial ownership during a corporate lifecycle, and, in the future, issuing digital securities.[383]

Stricter Bank Supervision in Emerging Nations

Money launderers do not respect borders. Financial Intelligence Units and law enforcement authorities have jurisdictional limitations and often lack resources. As a result, criminals can exploit jurisdictional gaps to circumvent AML national laws. The Financial Stability Board has recently recommended stricter bank supervision and financial crime law enforcement in developing nations to halt the decline in correspondent banking ("de-risking"). The FSB statement recognizes that many emerging countries have adopted AML laws but do not enforce them or lack capacity to adequately supervise banks. As a consequence, banks in the US and other developed economies, particularly in Europe, as per Bank of International Settlements statistics on July 2016, have increasingly withdrawn from doing business in high-risk jurisdictions.[384]

As the Comptroller of the Currency stated before the Institute of International Bankers in 2016: "if U.S.-chartered financial institutions have a clear understanding of the risks associated with their

383 Delaware Office of the Governor, "Governor Markell Launches Delaware Blockchain Initiative. Reflects State's Commitment to innovation and Embracing the New Economy," Press Release, May 2016, http://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html; see also Delaware Chancery Court Judge J. Travis Laster speech before the Council of Institutional Investors (Chicago), "The Block Chain Plunger: Using Technology to Clean Up Proxy Plumbing and Take Back the Vote," Council of Institutional Investors, September 2016, http://www.cii.org/files/09_29_16_laster_remarks.pdf.

384 Binham, "Stricter Bank Supervision Needed in Developing Nations, Say Policymakers."

correspondent banking clients and the jurisdictions in which they are located, they may be more comfortable providing banking services, even those services that may have historically had higher risk."[385]

International Cooperation

Recent successful international anti-corruption cooperation examples among law enforcement authorities include Odebrecht, Braskem, and International Soccer. As the US Justice Department announced in 2016 referring to sharing information among law enforcement authorities under the Foreign Corrupt Practices Act Pilot Program: "an international approach is being taken to combat an international problem."[386]

In the US v. Odebrecht case, the US jurisdiction was attracted via the use of US bank accounts by Odebrecht and Braskem in Miami. Odebrecht, a Brazilian conglomerate, engaged in 2001 in a scheme paying bribes to officials in several countries including Brazil, Angola, Argentina, Colombia, the Dominican Republic, Ecuador, Guatemala, Mexico, Mozambique, Panama, Peru, and Venezuela. The Justice Department called "an elaborate, secret financial structure" to pay $778 million in bribes over fifteen years. In exchange, Odebrecht asked politicians on retainer to pass friendly tax legislation and contracts with state-owned oil companies such as Petrobras.[387]

Braskem, a Brazilian petrochemical company, also participated in the scheme and received several contracts with Petrobras. Both companies pleaded guilty for corrupt payments and profits, which amounted to approximately $3.8 billion. The final penalty[388] for Odebrecht was determined to be $2.6 billion in April 2017 (initially estimated at $4.5 billion but negotiated down since Odebrecht admitted it could not pay the fine). Brazil would receive 80 percent of the recovery, with the United States and Switzerland receiving 10 percent each. Braskem pleaded guilty to violating the Foreign Corrupt Practices Act and agreed to pay a criminal penalty of $632 million. Brazil would receive 70 percent of it, with the United States and Switzerland receiving 15 percent each.

International cooperation mechanisms among law enforcement authorities and Financial Intelligence Units and exchange of information should be prioritized and reinforced. Another successful example of international anti-money laundering cooperation between the US Treasury and foreign governments was the US Treasury's declaration in October 2015 of Banco Continental (Honduras) Group as "specially designated narcotics traffickers," which allows the freezing of assets in the United States due to money laundering.[389] The Honduran authorities cooperated in the investigation and liquidated the Honduran bank, which had been involved in money laundering activities for a decade.

The Egmont Group is composed of a number of FIUs that have been working together since their first meeting in Brussels in 1995, at the Egmont-Arenberg Palace.[390] The group provides a forum for FIUs that allows them to share information through memoranda of understanding meant to improve anti-money laundering programs. The exchange of financial intelligence can generate evidence in fighting financial crime and improve FIU expertise.[391]

At the European level, the European Commission's recent proposal of 5AMLD would enhance the FIUs' authority to access information from any covered entity in Europe across national borders by setting up automated centralized mechanisms in the form of (i) a central data registry of holders of banking and payment accounts or (ii) central data retrieval systems.[392] The interconnection of central registries would also increase transparency.[393] Moreover, the recent proposal to set up a strong independent European Public Prosecutor's Office with authority over all types of financial crimes affecting the EU

385 Remarks by Thomas J. Curry, Comptroller of the Currency, March 7, 2016, https://www.occ.gov/news-issuances/speeches/2016/pub-speech-2016-25.pdf.

386 US Department of Treasury, "Treasury Announces Key Regulations and Legislation to Counter Money Laundering and Corruption, Combat Tax Evasion," Press Release, May 5, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0451.aspx.

387 Acting Assistant Attorney General Kenneth A. Blanco, "Statement at the American Bar Association National Institute on White Collar Crime" (speech, Miami, FL, March 10, 2017), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-kenneth-blanco-speaks-american-bar-association-national.

388 United States of America v. Odebrecht S.A., Plea Agreement, https://www.justice.gov/opa/press-release/file/919911/download

389 Gustavo Palencia and David Alire Garcia, "Honduran Bank at Center of Money Laundering Case to Be Shut Down," Reuters, October 11, 2015, http://www.reuters.com/article/honduras-crime-banking-idUSL1N12B0I820151012.

390 Egmont Group, *Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases,* June 2011.

391 See Egmont Group, *100 Cases from the Egmont Group,* http://www.egmontgroup.org/library/cases.

392 See 5AMLD approved by the EU Council, *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849.*

393 See proposed Measures 3 and 4 under the European Commission, *"Anti-Money Laundering and Counter Terrorist Financing: Stronger Rules to Respond to New Threats,* 2016, http://ec.europa.eu/justice/criminal/document/files/aml-factsheet_en.pdf, 2-4.

budget could be an important step in preventing financial crime.[394]

Independent Assessments for High-Risk Jurisdictions

Evaluating the money-laundering risk in several countries and jurisdictions requires looking at different sources. FATF identifies jurisdictions that have strategic AML deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.[395] Countries that are often in the media for corruption, drug trafficking, and terrorism generally qualify as high-risk jurisdictions. Most AML laws require banks to conduct enhanced due diligence processes for customers doing business in high-risk countries. Banks, governments, and private firms use data analytics tools to pool data when evaluating country risk. Country risk analytics tools generally use algorithms to weigh and process data gathered from public and private sources. When choosing data analytic tools, it is important that the data are comprehensive, accurate, and frequently updated.

Countries in sanctions lists published by the United Nations, the United States, United Kingdom, and European Union need to be monitored by global banks to avoid regulatory fines. Country reports and evaluations published by international financial institutions, such as the International Monetary Fund and the World Bank, are also useful information sources to assess country risk. A frequent source of information for country risk analysis is the US Department of State's global annual report on money laundering and financial crime, which provides country evaluations based upon the contributions of numerous US government agencies and international sources.[396]

In 2010, FATF issued guidance concerning how it would identify certain high-risk countries by describing specific strategic AML deficiencies. The FATF conducts mutual evaluations (peer-to-peer reviews) on member countries' compliance with respect to its recommendations. In February 2013, FATF developed a methodology for AML country assessments.[397]

The IMF has endorsed the FATF 2012 recommendations and 2013 methodology. The IMF's financial integrity reviews apply to selected cases of Article IV consultations (surveillance programs), which are similar to annual audits the IMF holds with each member state, as well as its Financial Sector Assessment Program (FSAP). FSAPs are in-depth examinations of the financial sector, conducted by the IMF (jointly with the World Bank in the case of developing nations), and are associated with an Anti-Money Laundering/ Counter-Terrorism Financing (AML/CTF) review. The IMF's 2012 Guidance Note sets out a number of criteria that guide staff in determining whether financial integrity issues should be included in the IMF's surveillance programs.[398] The Guidance Note refers to cases where money laundering, terrorism financing, and related crimes (such as corruption or tax crimes) are serious enough to threaten domestic stability, balance of payments stability, or the effective operation of the international monetary system.[399]

The IMF's corruption reviews could be adopted more broadly, as recognized by its managing director, based on good governance principles.[400] Ukraine is an example where the endemic corruption has prompted the IMF to work with the authorities to propose anti-corruption measures and agencies, change public procurement rules, dismantle a company, and reform the judicial system. These good governance measures agreed to by the authorities were part of the IMF's economic recovery plan for Ukraine.[401]

Increasing transparency requests from stakeholders and donors should make international financial institutions consider promoting financial integrity and good governance for financial assistance

394 See "Anti-Money Laundering, European Public Prosecutor's Office, Digital Contracts, and Insolvency," Speech by Commissioner Jourová to the Legal Affairs Committee and EU Affairs Committee in the Bundestag, September 26, 2016, http://europa.eu/rapid/press-release_SPEECH-16-3189_en.htm.

395 FATF, Public Statement, April 2017, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-february-2017.html

396 See US Department of State, *Volume II: Money Laundering and Financial Crimes*, 2016, http://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/index.htm.

397 FATF, *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems,* February 2013, http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.

398 International Monetary Fund, *Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism,* February 2014, https://www.imf.org/external/np/pp/eng/2014/022014a.pdf, 15, Sections 25, 26 and 27.

399 The IMF and the Fight Against Money Laundering and the Financing of Terrorism, May 2017, http://www.imf.org/external/np/exr/facts/aml.htm

400 Remarks by Christine Lagarde, "The Power of Transparency to Increase Economic Resilience," at the Atlantic Council, February 8, 2017, https://www.youtube.com/watch?v=1ifk0OZMPvo.

401 Ibid.

programs[402] based on: (i) the global reach of negative spillover effects of corruption, illicit financial flows, and trade-based money laundering; (ii) the increasingly global reach of virtual currency businesses (such as virtual currency exchanges and e-wallets), and the anonymity risk they represent as potential facilitators of illicit activities; and (iii) the recent recommendations by the Financial Stability Board for developing nations to strengthen bank supervision to halt de-risking in correspondent banking activities.

How To Help Government and Law Enforcement with Oversight Responsibilities

Expand the Use of Regtech, Automated Data Analytics, and Monitoring Systems

The Basel Committee report on sound management of risks related to money laundering and financing terrorism also recommends using automated risk analytics tools at a global level: "For most banks, especially those which are internationally active, effective monitoring is likely to necessitate the automation of the monitoring process. When a bank has the opinion that an IT [information technology] monitoring system is not necessary in its specific situation, it should document its decision and be able to demonstrate to its supervisor or external auditors that it has in place an effective alternative. . . . The IT monitoring system should enable a bank to determine its own criteria for additional monitoring, filing a suspicious transaction report (STR) or taking other steps in order to minimize the risk."[403]

The financial sector's obligation to report suspicious activities to a Financial Intelligence Unit exists in many countries. Technology is helping the financial sector analyze, filter, investigate, and process information on suspicious transactions. This should be complemented with regular training programs for employees. Most global banks have incorporated automated tools to help them comply with STRs and other regulatory or disclosure requirements. Whether they purchase software from vendors or develop their own monitoring programs, the important thing is to get the job done in capturing unusual client behavior patterns. US and EU financial crime enforcement

"Technology is helping the financial sector analyze, filter, investigate, and process information on suspicious transactions."

authorities expect to test the technology during inspection visits to determine whether the system appropriately detects suspicious transactions. Given technological advances and the decreased cost of available systems, it would be difficult today for any US bank to claim that it is reasonable to rely on a largely manual system to identify and report suspicious transactions to authorities.[404]

Multi-stakeholder Processes

Other countries should consider following the UK's lead in creating task force groups and opening channels of communication with the financial sector.[405] Such task force groups leverage intelligence that banks may have when conducting global business, beyond formal STRs reporting. Channels for direct dialogue between the financial sector and governmental agencies can prove mutually beneficial.

Public-private partnership initiatives (PPPIs) are often led by international financial institutions in partnership with international banks, government agencies, and the private sector to boost investments in the energy, water, infrastructure, and transport sectors. As the lead adviser, international financial institutions work with governments on legal and regulatory requirements to build technical capacity. International financial institutions should consider including financial integrity safeguards, similar to environmental and social safeguards, in their design of the PPPI strategies. These are key to fostering transparent bidding processes and good governance and to avoiding corruption. Implementing these safeguards would also have the benefit of raising financial integrity standards for local partners.

402 AML/CFT measures have been incorporated into conditionality under fund-supported programs in Afghanistan, Cyprus, Greece, Kyrgyzstan, São Tomé and Príncipe, and Uganda. See International Monetary Fund, *Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism,* February 2014, https://www.imf.org/external/np/pp/eng/2014/022014a.pdf, 17.

403 Basel Committee on Banking Supervision, "*Sound management of risks related to money laundering and financing of terrorism,*" (Basel, 2016), 6-16.

404 US Department of the Treasury Financial Crimes Enforcement Network, in re: "*Eurobank, San Juan, Puerto Rico*," (No. 2010-2), https://www.fincen.gov/sites/default/files/enforcement_action/AssessmentEurobank.pdf, 4; See also Financial Industry Regulatory Authority, *Anti-Money Laundering*, Special NASD Notice to Members 02-21.

405 Jonathan Pickworth and Jonah Anderson, "New UK AML Action Plan – The Increased Role of the Private Sector," White & Case, April 28, 2016, http://www.whitecase.com/publications/alert/new-uk-aml-action-plan-increased-role-private-sector.

Voluntary Standards

The Wolfsberg Group is an example of how collective action from global banks can help promote strong international AML standards. Although the group has been criticized for being too formalistic and relying too much on information based on standard questionnaires, it is also recognized that these questionnaires have simplified the due diligence process for correspondent banking through data repositories. In addition to formal AML policies, the group should consider analyzing the efficiency of the automated controls currently in place to detect and monitor suspicious transactions and clients.

FATF recommendations have not been fully implemented in many countries and global banks face challenges operating in countries with weak financial crime regulations or enforcement. The Financial Stability Board has called on developing nations to adopt stricter banking supervision rules to halt the decline in correspondent banking relationships (de-risking).[406] Global correspondent banks can have a positive influence raising local standards to avoid de-risking, and creating incentives for local banks to voluntarily adopt higher AML standards, even if not required by local AML laws. Global asset managers and large pension funds can play a role in raising the corporate governance standards of the companies they invest in at a global level.

Recommendations

The following proposals could help underpin financial integrity if adopted at a global level:

- The Financial Stability Board, FATF, and regulators should work together to ensure that transparency exemptions for risk management and security purposes are addressed in privacy and other relevant laws to enable information-sharing regimes.
- The FSB should promote global regulatory coordination for the improvement of data formats and standardization of financial definitions for risk data aggregation.
- The FSB should develop international standards and best practices addressing cybersecurity.
- The FATF should provide clear definitions of key regulatory concepts and guidelines, such as Know Your Customer regulations or digital client onboarding due diligence.
- Financial regulators should promote the use of data analytics and monitoring tools by banks and their gatekeepers and fintech companies.
- Banks and supervisors should review rules that may hinder regtech experimentation.
- Emerging countries should reinforce financial supervision and explore technology innovation such as the issuance of digital identities to promote financial inclusion.
- International financial institutions should expand their role in promoting good governance programs and the adoption of FATF recommendations.
- Financial Intelligence Units should reinforce international cooperation and set up public-private task force groups to exchange informal intelligence.

Conclusion

Data analytics tools used by the public and private sectors to fight financial crime need high-quality and accessible data at a global level. Data protection or localization rules create obstacles to accessing data and sharing information across financial groups and lead to "silos" of information, against the Basel Committee's principles for effective risk data aggregation and reporting.[407]

As a result, for automated tools to effectively mitigate financial crime risks, privacy laws should include exemptions for data sharing based on transparency and security purposes. For instance, many jurisdictions, including the European Union, which has implemented FATF recommendations, require consent for processing personal data. Such privacy laws pose potential risks to accessibility and data quality, which are necessary to fight financial crime. The Financial Stability Board, FATF, and regulatory authorities should engage in international dialogue to favor certain risk-based exemptions for data sharing, permitting the processing and disclosure of personal data without a data subject's consent, to prevent fraud and corruption or for money laundering risk control. The Financial Stability Board should also intensify efforts for global regulatory coordination to improve standardization of data formats on financial concepts and definitions. A lack of data harmonization or insufficient detail of definition makes it hard to aggregate risk data across financial groups and jurisdictions on an automated basis.[408]

406 See Binham, "Stricter Bank Supervision Needed in Developing Nations, Say Policymakers."

407 Basel Committee on Banking Supervision, *Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, February 2016, http://www.bis.org/bcbs/publ/d353.pdf.

408 Institute of International Finance, Regtech in Financial Services: Technology Solutions for Compliance and Reporting, March 2016, p. 4, https://www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting

The FATF 2012 recommendations have not been enforced, or not fully enforced, in many countries. Such regulatory asymmetry creates gaps, which favor the circumvention of financial crime laws by moving the activities to jurisdictions, to the digital economy, or to unregulated sectors. To mitigate such risks, banks and other relevant players need to effectively use data analytics tools to monitor clients and transactions, and share intelligence with FIUs. Gatekeepers and new digital finance businesses (such as virtual currencies exchanges, money services businesses, and online lending platforms), should use automated data analytics tools, have effective AML frameworks, and report suspicious transactions, even on a voluntary basis. Emerging countries should explore regtech solutions such as digital identity to promote financial inclusion. They should also focus on stricter supervision of banks to avoid "de-risking," according to FSB. International financial institutions' role should be more prevalent in promoting good governance and financial integrity, consistent with FATF 2012 and Basel Committee recommendations. Financial Intelligence Units and law enforcement authorities should reinforce cooperation and exchange of information mechanisms at a global level, including public-private partnerships and task force groups.

Technological innovation, such as regtech and smart contracts, has the potential to effectively help banks streamline regulatory compliance processes and facilitate effective supervision by authorities. As an example, the global AML/CTF framework lacks universal definitions of key concepts, such as Know Your Customer or client due diligence requirements. National identification documents also vary from country to country. Placing KYC utilities on a distributed ledger could allow banks to share sensitive consumer data across several entities, facilitating KYC and supervision, without compromising nonpublic personal data (although it would not solve all the issues concerning data sharing). To mitigate the risk of experimenting with new technologies, regulators should set up an open dialogue with banks and start-ups to promote a "safe" environment and experimentation, where both supervisors and firms can work together to analyze how regulations can unintentionally impact automation and innovation, such as through requiring in-person identification instead of allowing digital identity verification methods.[409]

Fintech and regtech technologies that monitor customer activities may also increase cybersecurity and privacy risks.[410] Anytime an organization collects customer data, it must ensure that it preserves data from cyberattacks.[411] Regulators should change their supervisory focus as digitization changes the types of risk in the financial sector, shifting to cybersecurity risk. Ultimately, regulators need to set up international standards addressing legitimate privacy and cybersecurity concerns, while at the same time ensuring transparency and financial integrity, through dialogue with the private sector and the creation of new mechanisms to promote coordination among relevant agencies internationally to fight financial crime, protect data privacy, and uphold information security.

409 Institute of International Finance, Deploying Regtech against Financial Crime, March 2017, https://www.iif.com/system/files/32370132_aml_final_id.pdf, 27.

410 Citi Global Perspectives and Solutions, *E-Privacy and Data Protection: Who Watches the Watchers? How Regulation Could Alter the Path of Innovation,* March 2017, https://ir.citi.com/l%2FDe1TjhFWX1NpgDsXKJmsACj6DaypITsS7sNZ8DtTZvNvVHwHlNTmLogXdvmMMu727lshzkyVo%3D.

411 Kevin Petrasic, Benjamin Saul, and Helen Lee, "Regtech Rising: Automating Regulation for Financial Institutions," White & Case, September 16, 2016, https://www.whitecase.com/publications/insight/regtech-rising-automating-regulation-financial-institutions.

AUTHORS

Chapter 1

Els De Busser, *Senior Lecturer, European Criminal Law; Senior Researcher, Centre of Expertise Cyber Security*, The Hague University of Applied Sciences

Els De Busser holds a Ph.D. from Ghent University, Belgium and is currently senior lecturer at the Faculty Public Management, Law & Safety and senior researcher at the Faculty IT & Design, Centre of Expertise Cyber Security of The Hague University of Applied Sciences, the Netherlands. She is guest researcher at Leiden University, Institute of Security and Global Affairs; a member of the Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee); secretary of the Scientific Committee of the International Association of Penal Law (AIDP) and expert for the European Judicial Training Network (EJTN). Her research is focused on European and international cooperation, cyber security, information exchange, and data protection in criminal matters especially in the transatlantic relationship. She is a frequent speaker at international events and guest lecturer on these topics. Her book "Data Protection in EU and US Criminal Cooperation" (Maklu, 2009) was awarded with the 2014 Siracusa Prize for Young Penalists by the Association Internationale de Droit Pénal (AIDP) and the International Institute of Higher Studies in Criminal Sciences (ISISC).

Chapter 2

Erica J. Briscoe, *Chief Scientist ATAS Laboratory*, Georgia Tech Research Institute

Erica J. Briscoe is a Senior Research Scientist and a Lab Chief Scientist at the Georgia Tech Research Institute (GTRI) in Atlanta, GA. She oversees basic research and development projects focused on behavioral and data science/analytics applications in various problem spaces, including: computational social science, technology emergence and prediction, social network analysis, insider threat detection, terrorism and radicalization, business intelligence, and psychological profiling. Dr. Briscoe received a BS degree in Industrial Engineering from Georgia Tech, an MS degree in Information Systems from Drexel University, and an MS and PhD from Rutgers University in Cognitive Psychology.

Chapter 3

Benjamin C. Dean, *President*, Iconoclast Tech

Benjamin C. Dean works at the intersection of technology, economics and public policy. He is President of Iconoclast Tech, which advises clients on the economic, political and social implications of waves of technological change. He is also presently a Ford/Media Democracy Fund Technology Exchange Fellow at the Center for Democracy and Technology in Washington DC. Previously he was a fellow for cybersecurity at Columbia University and a policy analyst at the Organisation for Economic Co-operation and Development (OECD). Currently, Mr. Dean contributes to an initiative to develop business digital risk management metrics at the OECD's Working Party on Security and Privacy in the Digital Economy. He recently contributed a paper to inform the European Parliament on the economic implications of EU-US cooperation in cybersecurity and cybercrime. He also assists re-insurance clients with the development of models to assess the probability and impact of a variety of digital security incidents. Mr. Dean completed a MA International Affairs at Columbia University's School of International and Public Affairs. He is also a graduate of the University of Sydney with a BA Economics and Social Sciences (Hons.)

Chapter 4

Tatiana Tropina, *Senior Researcher*, Max Planck Institute for Foreign and International Criminal Law

Tatiana Tropina is a senior researcher at the Max Planck Institute for Foreign and International Criminal Law. Her current areas of research include international standards to fight cybercrime, the comparative analysis of cybercrime legislation, self- and co-regulation, public private partnerships to address cybersecurity issues, cybersecurity and human rights, and the multi-stakeholder approach to fight cybercrime. Tatiana's background includes both academic and practical experience. She has been conducting cybercrime research for 15 years, starting in Russia in 2002, where she became the first Russian researcher to defend a PhD thesis on cybercrime (2005). From 2002 to 2009, she was responsible for cybercrime projects at the regional subdivision of the Transnational Crime and Corruption Centre (George Mason University, USA) in Vladivostok, Russia. At the same time, from 2003 to 2008, she worked full-time as a lawyer and then as head of the legal departments of a number of telecommunication companies. Since 2009, Tatiana Tropina has been involved in both legal research and various applied cybercrime projects at the international level.

Chapter 5

Miren B. Aparicio, *Counsel and Senior Consultant*, The World Bank Global Practice

Miren B. Aparicio is a counsel and senior consultant at the World Bank Global Practice and a member of the Chamber of Digital Commerce Smart Contracts Alliance initiative in Washington DC. Ms. Aparicio has advised financial services firms in a wide range of investment banking business sectors. Her practice focuses on Fintech and Regtech, capital markets and financial crime, including policy and regulatory advise for governments. Ms. Aparicio's financial services experience in Spain includes working at Morgan Stanley (as General Counsel and Head of Compliance), Société Générale Corporate and Investment Banking and BBVA. Ms. Aparicio developed an Anti-Money Laundering and Counter-Terrorism Financing institutional framework, risk mitigation and governance for the Inter-American Development Bank. Her publications include several articles with Thomson Reuters regulatory intelligence (Accelus) about the need to balance Fintech innovation and regulation. Ms. Aparicio is an LL.M. graduate at Columbia University of New York; D.E.A. in International Law at the Graduate Institute of International Studies in Geneva; Certified Anti-Money Laundering Specialist (CAMS).

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org