16. Embedded extraterritoriality: US judicial litigation and the global banking surveillance of digital money flows[1]

Grégoire Mallard and Anna Hanson

1. INTRODUCTION

Following the terrorist attacks of 9/11 and the revelation of Iran's secret nuclear programme, North American and European government officials and those working in law enforcement began emphasizing the importance of financial datamining in combating terrorism and nuclear proliferation. There was a growing belief that financial data could be used as a way to prevent terrorist attacks and that increased financial transparency requirements would discourage global banks from keeping and managing the money of customers designated by the United Nations Security Council (UNSC) for their role in the illicit nuclear programmes of Iran or North Korea. Law enforcement and regulators came to view financial information as far more reliable than other forms of intelligence when it came to conducting post-hoc analysis of sanctions violations and convincing global banks that the risks of detection were too high for them not to care about the international community's efforts to combat either terrorism or nuclear proliferation.[2] As then US Treasury Secretary John Snow argued, 'money trails don't lie'.[3] Those banks that accompanied the change constantly updated their practice by co-opting the datamining technologies that they had been using for commercial purposes in order to profile their customers and determine client profitability in order to help pinpoint, amongst millions of financial transactions, the few suspicious withdrawals and transfers that could potentially indicate terrorist or WMD financing: these banks were the 'good citizens' of the banking community, in contrast to the 'bad banks' that resisted the idea of increased transparency through mass surveillance of digital transactions and the automatic exclusion of suspicious clients and the freezing of their assets.[4]

This chapter goes back over this narrative, by exploring the implications of banks adopting US based financial data-management software programs in their affiliates. Based on in-depth interviews with former US government officials (Treasury, State) as well as transnational

[1] This chapter is directly based on a project headed by Grégoire Mallard that received funding from the European Research Council under the European Union's Horizon 2020 research and innovation programme (Grant Agreement PROSANCT, 'Bombs, Banks and Sanctions' Project 716216). The authors thank all the interviewees who participated in the research.

[2] Thomas Biersteker, Sue E Eckert and Marcos Tourinho (eds.), *Targeted Sanctions: The Impacts and Effectiveness of United Nations Action* (Cambridge University Press 2016).

[3] Cited in Marieke de Goede, *Speculative Security*: *The Politics of Pursuing Terrorist Monies* (University of Minnesota Press 2012), 58.

[4] Juan Carlos Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (Public Affairs 2013).

regulatory bodies like the World Bank and the International Monetary Fund (IMF), and compliance officers working in global banks, it studies how compliance officers in global banks understand the logic of sanctions in general, and the role that 'financial instruments'[5] and other software programs play in shaping due diligence checks. In particular, this chapter questions how the notion of 'extraterritoriality' of sanctions is conceived in practice. This chapter thus asks: How do compliance officers in global banks perceive the risks associated with violations of US sanctions law? Do we observe a trend towards sanctions accumulation whereby global banks 'over-comply'[6] by observing all US and European sanctions in their worldwide activities, irrespective of the territory in which transactions take place? If so, what are the monitoring systems in place that drive global banks' compliance officers to give priority to worldwide compliance with US law? Are there alternatives to US based software companies, and if so, is there a market for financial institutions able or willing to conduct business in regions that have rejected the use of these software programs?

In asking these questions, this chapter focuses on the 'socio-technical embeddedness'[7] of US extraterritoriality. In particular it seeks to answer the question of who leads the change in transparency requirements within banks, and whether the recent global trends towards overcompliance with US sanctions law are the result of the community's internal efforts to establish a more 'ethical' standard of practice and global adhesion to the current programme aimed at countering the financing of terrorism (CFT), counter-proliferation financing (CPF) and anti-money laundering (AML) promoted by the United States and its allies; or whether other logics are at stake, including the aggressive extraterritorial projection of US sanctions law onto the global playing field in which global banks operate through a series of harsh enforcement actions.

As regards method and theory, this chapter is situated in an interdisciplinary conversation with anthropologists of finance[8] and socio-legal scholars[9] who focus on the mundane practices of banking. In this instance it focuses on the work of back-office employees, who, as Annelise Riles once remarked, receive much less attention than the speculative – or at least calculative – practices of the traders whose scandalous bonuses have become objects of adoration or shame since the financial crisis of 2008.[10] Compared to trading floors, the banks' compliance offices remain one of those black-boxes in the anthropology of finance that have seldom been

---

[5] Karin Knorr Cetina, 'Financial Analysis: Epistemic Profile of an Evaluative Science' in Charles Camic, Neil Gross and Michèle Lamont (eds.), *Social Knowledge in the Making* (University of Chicago Press 2011) 405–41.

[6] Grégoire Mallard, Farzan Sabet and Jin Sun, 'The Humanitarian Gap in the Global Sanctions Regime: Assessing Causes, Effects and Solutions' (2020) 26(1) Global Governance: A Review of Multilateralism and International Organizations 121–53.

[7] Donald MacKenzie, *An Engine, Not a Camera: How Financial Models Shape Markets* (MIT Press 2006).

[8] Donald MacKenzie, Fabian Muniesa and Lucia Siu, 'Introduction' in Donald MacKenzie, Fabian Muniesa and Lucia Siu (eds.), *Do Economists Make Markets? On the Performativity of Economics* (Princeton University Press 2007) 1–19.

[9] Terence Halliday and Bruce Carruthers, 'The Recursivity of Law: Global Norm Making and National Lawmaking in the Globalization of Corporate Insolvency Regimes' (2007) 112(4) American Journal of Sociology 1135–202.

[10] Annelise Riles, 'Collateral Expertise: Legal Knowledge in the Global Financial Markets' (2010) 51(6) Current Anthropology 795–818.

opened by ethnographers who draw on the Science and Technology Studies (STS) literature[11] to analyse the practices of hedge fund managers and other high-powered individuals who abide by the 'code of finance'.[12] In so doing this chapter responds to Annelise Riles' call to 'broaden the frame of the market to include what is on the margins' and thereby leave 'the more glamorous front office, where well-paid traders revered for their financial genius or their wizardlike intuition about markets work their computer screens and telephones', and instead enter into 'the back office and [talk to] its employees who exist to supply the legal infrastructure for the trades'.[13]

The back office is an interesting place for anthropologists of finance and socio-legal scholars because it is a highly regulated place, and sometimes even a highly judicialized place, especially for the global banks that have agreed to host monitors on their floors after signing Deferred Prosecution Agreements (DPAs) with the US Department of Justice as a result of a series of landmark sanctions enforcement actions launched in the last 15 years by the Office of Foreign Assets Control (OFAC) in the US Treasury Department.[14] Filing reports about the good ethics and professional standing of their clients, the level of reputational risks that their clients represent for the bank, reporting suspicious transactions to regulatory agencies hosted in Ministries of Finance and Departments of the Treasury, as well as undergoing regular examinations that evaluate bank activities and management processes, including the robustness of compliance/sanctions programmes, the men and women in compliance offices are asked to perform an increasingly wide range of tasks that fall under the broad provisions of Know Your Customer (KYC) and other due diligence compliance guidelines. Insisting on the 'ethical dimension' of the job of compliance officers, Bill Maurer notices that the term 'bears a family resemblance to the pastoral discourse of harm and explicitly invokes ethical conduct',[15] or more precisely, an 'ethics of care' which is generally portrayed as belonging to the realm of relational work rather than the competitive and aggressive world of trading. But rather than looking at the performance of compliance officers from the ethical point of view, this chapter investigates whether new practices in the field of compliance, especially practices related to the use of new software technologies, have had an effect in extending the reach of US sanctions law beyond the US borders.

The extraterritoriality of US law, this chapter argues, is embedded in the daily practices of the back offices of global banks. Decisions to conform to US sanctions law outside the US jurisdiction are taken on a routine basis in such a context, which is also shaped by the global banks' general guidelines and appetite for risk, but also by the way financial management software is programmed. Decisions to block transactions, freeze assets or report suspicious

---

[11] For a similar inspiration from STS to study the practices of sanctions, see de Goede (n 3); Gavin Sullivan, *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law* (Cambridge University Press 2020).

[12] Vincent Lepinay, *Codes of Finance: Engineering Derivatives in a Global Bank* (Princeton University Press 2011).

[13] Riles (n 10) 797, 798.

[14] Grégoire Mallard, 'Governing Proliferation Finance: Multilateralism, Transgovernmentalism and Hegemony in the Case of Sanctions Against Iran' in Eric Brousseau, Jean-Michel Glachant and Jérôme Sgard (eds.), *Handbook of Institutions of International Economic Governance and Market Regulation* (Oxford University Press 2019).

[15] Bill Maurer, 'Due Diligence and "Reasonable Man", Offshore' (2005) 20(4) Cultural Anthropology 474–505, 477.

transactions are the kind of qualitative assessments that are now part of the routine work of compliance departments whose practical logic has been shaped by OFAC's interpretation of US regulatory obligations on global banks with an office in New York. So this is the world in which the question of the extraterritoriality of US sanctions is addressed in actual practice. Thus, by studying the world of compliance in banking in general and the embeddedness of US extraterritoriality in practice, our chapter moves away from a narrow focus on the purely legal analysis of the jurisprudence built by the series of OFAC sanctions cases since 2005, or the series of de-listing cases brought before the European Court of Justice by either individuals accused of financing terrorism,[16] or Iranian banks accused of funding proliferation.[17]

As the chapter shows first, the world of compliance in global banks has been radically changed by the DPAs that the US government and New York (NY) state offices have forced banks to sign after they were found to be in violation of the US sanctions imposed against Iran after 2008. One should thus go beyond the idyllic vision of 'ethical' global banking practices and analyse the routinization of KYC practices and due diligence in a context in which global banks did not originally wish to make their operations more transparent to the gaze of the regulators, especially the US regulators. Compliance officers have been asked by the US executive to rely increasingly on software technologies that would enable them to screen billions of transactions and identify patterns that could help them defend the 'integrity' of their banks against their potential hijacking by professional money launderers, sanctions busters or proliferation financiers. The routinization of compliance has thus been largely automated. The next sections explain how the new compliance practices developed in this altered context did not particularly correspond to compliance officers' own understanding of what constituted good ethical work – but that in the context of massive fines being extracted by the United States from European banks, they preferred to adopt a form of 'blind proceduralism'[18] and engage in other forms of 'non-knowledge' that could help protect their (ir-)responsibility in the event of reported violations of the new rules.

2. THE POWER OF US HARD LAW: WHY GLOBAL BANKS ADOPTED NEW SOFTWARE TECHNOLOGIES IN THE 2010S

The growth of the compliance sector in banking has been spurred not only by the 'ethical' AML campaign launched in the 1990s against drug cartels and financial crooks but also by the global sanctions programme against Iran's nuclear development, which started in the 2000s. For more than a decade, legal rules have been added at all levels of governance from which

[16] Daniel Halberstam, 'Local, Global and Plural Constitutionalism: Europe Meets the World' in Grainne De Burca and Joseph Weiler (eds.), *The Worlds of European Constitutionalism* (Cambridge University Press 2010); Charlotte Beaucillon, *Les mesures restrictives de l'Union européenne* (Bruylant 2014).

[17] Jin Sun, Grégoire Mallard and Charlotte Beaucillon, 'Judicial Remedies to Tame the Hegemon? The Legal Battle in Europe Around the Iran Nuclear Deal' (Manuscript under review, Graduate Institute, May 2021).

[18] Grégoire Mallard and Linsey McGoey, 'Strategic Ignorance and Global Governance: An Ecumenical Approach to Epistemologies of Global Power' (2018) 69(4) British Journal of Sociology 884–1055.

a global system of surveillance of the financial dealings of *all* states, banks and individuals, has emerged. Since 9/11, new international institutions have multiplied in the field of banking regulation, and their activity, particularly that of the United Nations Security Council (UNSC) Sanctions Committees and the Financial Action Task Force (FATF), has involved many legal experts from a wide range of countries.[19] This is a new and unprecedented development in the transnational governance of money: the UNSC, FATF, IMF, Egmont Group (an association of national financial intelligence units) and transnational networks of legal and financial specialists working to produce expertise on financial regulatory practices do not only produce new 'rules', 'best practices' and norms that now form part of the new transnational legal order concerned with the regulation of money flows, but they also work to buttress the legitimacy of new 'regulatory infrastructures' which facilitate 'the flow of goods, services, people, money, data, information, practices, and ideas over physical or virtual space'.[20] Money flows between global banks are now called on to become digitally transparent in the hope that banks can more easily comply with the new banking regulations arising out of the transnational and international financial institutions in charge of AML, CFT or CPF.

The process of digitalization of money flows is not only embedded in a 'transnational legal order'[21] or an architecture of 'transnational governance'[22] but also in deeply domestic legal requirements which one country – for example, the United States – has imposed on all banking institutions, domestic and foreign. The process, which aimed at exposing private financial transactions of global banks to the gaze of US authorities, started when US enforcement agencies from the Treasury Department and other judicial authorities went after the 'bad banks' that were involved in illegal practices, especially, but not only, those global banks that had hidden illicit transactions with Iran. As Juan Zarate, former Deputy National Security Advisor for Combating Terrorism, has stated in his memoirs:

> We had realized that a new banking ecosystem has emerged. This was now an environment in which banks were acutely sensitive to their reputation and the risks of doing business with suspect individuals and entities under the international regulatory and enforcement microscope. Banks were willing to cut financial and commercial relations with rogue regimes, criminals, and terrorists, given the right conditions … this new ecosystem also relied on a globalized financial infrastructure. This system connected all international actors – states and non-states – with its leading node in the United States – New York. New York serves as the most important financial center in the world, and the dollar serves as the global reserve currency and dominant currency for international trade, including oil. The twenty-first century financial and commercial environment had its own ecosystem that could be leveraged uniquely to American advantage.[23]

From 2009 to 2015 there were over 27 sanctions busting cases brought by either the Treasury's OFAC, the Justice Department or the New York Department of Financial Services (DFS) run by Benjamin Lawsky. What is also worth noting, is that within these sanctions busting cases,

---

[19] Mallard (n 14).

[20] Benedict Kingsbury and Sally Engle Merry, 'InfraReg Project' (2018) <www.iilj.org/infrareg/infrareg-project/>.

[21] Terence Halliday and Gregory Shaffer, *Transnational Legal Orders* (Cambridge University Press 2014).

[22] Marie-Laure Djelic and Sahlin Andersson (eds.), *Transnational Governance: Institutional Dynamics of Regulation* (Cambridge University Press 2006).

[23] Zarate (n 4) 150.

there was a fairly wide range of illicit activity. For instance, in 2012 HSBC was forced to pay $1.92 billion as part of its deferred prosecution agreement, which accused the bank of not only transferring billions of dollars for sanctioned nations such as Iran, but enabling Mexican drug cartels to move money illegally through the bank's American subsidiaries.[24]

These sanctions-busting cases took on new relevance after the US government and its specialized agency – the enforcement arm of OFAC – decided that it would consider it illegal from then on if banks cleared USD-denominated US-sanctionable transactions even if the latter involved no US citizen and took place outside the US: described as operating a 'U-turn', the money that moved for one fraction of a second in the US local branch – most often in New York – where these transactions were cleared placed the whole transaction under direct US jurisdiction, according to OFAC. This decision to link US-denominated transactions worldwide to claims of US judicial jurisdiction really marked the beginning of the trend towards the extraterritorial application of US sanctions law. As an expert in banking compliance told us during an interview, this doctrine, which was made official in a 2008 statement by OFAC, emerged earlier with a case against the Dutch ABN Amro bank:

> The real tipping point that changed the way the world looked at the global impact of US sanctions was the enforcement taken against ABN Amro Bank in December of 2005. This was the first significant OFAC-related enforcement action involving a non-US financial institution … The theory that was developed and used as the basis for asserting that violations of sanctions had occurred because ABN Amro had sent US dollar payments on behalf of Iranian banks and sanctioned Libyan banks through US correspondent banks was that ABN Amro had involved its own New York branch in the processing of those payments. And therefore, the New York branch had violated [US] sanctions even though the New York branch had no idea that the [US] sanctions applied because the payment messages were structured not to reference clients of the Dubai branch of ABN Amro, which happened to be Iranian banks and the one sanctioned Libyan bank … I refer to it as a primitive case because there was no assertion by anybody that the Dutch bank ABN Amro's Dubai branch had violated the sanctions. The theory was that the New York branch had violated the sanctions even though it was ignorant of the sanctions issues at the time it processed the payments. That case led to, sort of, a revolution in banking about the obligation of financial institutions globally to ensure that their US dollar payment activity complied with sanctions requirements. Prior to that point of time, there was a nearly universal absence of recognition of the risk.

Still, during the Bush years, penalties imposed by OFAC for Iran sanctions violations on European banks, such as ABN Amro and Deutsche Bank, were moderate compared with future fines imposed on BNP-Paribas or Standard Chartered. For example, for ABN Amro's suspected money laundering problems in Iran and Libya, OFAC's fine was US $80 million, which was roughly the same as the fines imposed on Citi and Wells Fargo when OFAC later found these two US banks to have similar problems. As the same interviewee continues:

> There had been some discomfort post-9/11 and prior to the ABN Amro case among some of the more far-sighted and ethically-minded non-US bankers about the use of non-transparency to disguise some US correspondent banks. The transactions involved sanctions targets because some of these methods were egregious. There was manipulation of message content to make a payment that involved Iran look like a payment that did not involve Iran. And it was considered acceptable practice primarily because there was a view in the industry that the prevailing standard, was 'don't ask, don't tell'. We

[24] Jessica Silver-Greenberg and Ben Protess, 'A Grieving Father Pulls a Thread That Unravels BNP's Illegal Deals' (*New York Times*, 30 June 2014).

> won't – US banks won't ask if these payments involved sanctions targets and we, the non-US banking community, won't tell them. This created what I call an 'enforcement trap' for the non-US banking community because based on this sentiment that the standard was 'don't ask, don't tell', many non-US banks created very deceptive means of not telling … by deliberately concealing information that viewed from the perspective of US authorities and US banks was relevant for their compliance.

For compliance officers, the ABN Amro case and the subsequent theory that it normalized afterwards, did not primarily involve any notion of extraterritoriality, even if policymakers later saw that its implications were that US law had extraterritorial effects. For OFAC, whether global European banks deliberately violated the US sanctions, or whether they missed the violations and failed to engage with enough pro-active drive, was a purely US problem, as the problem started for these global banks when the transaction was cleared in US territory, more specifically, in the New York branch of that global bank. Whether the global bank needed to start a complete overhaul of its sanctions programme or not was a different question, and in many ways, the response to the US problem raised by the question of clearing US dollars for a global bank found in violation of US sanctions law could have been solved without any implications for its non-US branches. A global bank could have reformed only its compliance practices in the NY branch, agreed to stronger monitoring requirements only in that branch, and imposed watertight distinctions between euro-denominated transactions following European (and not US) sanctions law. This is what many, but not all, global banks started doing in order to continue engaging in business with US sanctioned jurisdictions like Iran, at a time when it was still legal in Europe to commerce with that country in the profitable oil business, which was not prohibited in Europe until 2012.

But the penalties and conditionalities imposed on European global banks after the 2008 election of President Obama and the economic crisis completely changed in magnitude in the next wave of judicial settlements in the 2012–2013 period, and, in so doing, changed the European banking sector's perception of the motivations behind OFAC's new form of 'financial warfare' against European banks. One of the reasons for that change is the realization by OFAC that European banks were sometimes actively deceiving US regulators by either enrolling their NY branch in a vast conspiracy to hide US sanctionable transactions denominated in US dollars that were still being cleared in NY, or by not disclosing to their NY branch the true activities of non-US transactions. After 2012, in the cases against HSBC and BNP Paribas, European banks were required to forfeit the volume of money transfers involved in sanctions violations, as well as pay civil penalties for their AML procedural programme violations, by which one meant that banks had to send payments to a subject fund for any US and alien victims in any future civil compensation. Of all the global banks investigated, the only bank continuing U-turn practices related to Sudan and Iran after OFAC's November 2008 decision to make it a sanctionable crime was BNP Paribas, and it was the one on which maximum US pressure was brought, as it was the only instance that led to a court trial and guilty pleas by executives, whereas all other cases were settled before they got to court.[25]

These settlements responded to OFAC's demands that global banks (mostly headquartered in Europe) adopt a comprehensive and global overhaul of their compliance programmes – and

[25] OFAC (Office of Foreign Assets Control, U.S. Treasury Dept.). 'BNP Paribas Deferred Prosecution Agreement' (2014) <www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140630_bnp_settlement.pdf>.

not just the compliance programme of their New York branch – so that when these banks moved foreign money into US territory, even for a fraction of a second, the technologies of data management with which they operated worldwide would be reconfigured in such a way that compliance officers could no longer hide the origins, destination or purpose of those funds. In the United States, this is referred to as the 'Travel Rule' and is part of the Bank Secrecy Act (BSA) that requires all transactions of US $3000 or more to include all required information (Originator, Beneficiary, etc.) in the wire message.[26] A similar rule was adopted by the Financial Action Task Force (FATF) in 2012 with their Recommendation 16, which states that financial institutions have to provide information about the originator of a payment as well as the beneficiary.[27] This recommendation forces banks to closely monitor the quality of data in the transactions they receive.[28] It is supposed, for instance, to make it impossible for banks like Standard Chartered to secretly process thousands of transactions for Iranian clients through its American subsidiaries. In order to avoid having Iranian transactions detected by Treasury Department computer filters, Standard Chartered deliberately removed names and other identifying information. According to the Statement of Facts that was submitted in evidence, in early 2001, the Central Bank of Iran requested that Standard Chartered act as its correspondent bank for all US dollar transactions including payments relating to oil sales by the National Iranian Oil Company. As part of the agreement, the Central Bank of Iran instructed Standard Chartered to remove any reference to Iran in the SWIFT payment messages that went through New York.[29]

In the judicial settlements that were reached with most of these global banks, in addition to harsh penalties, the dismissal of senior executives and compliance officials, and the acceptance of huge rises in compliance costs by the banks, the prosecuting parties also insisted that new technologies should be adopted by global banks to avoid the same mistakes being repeated and further sanctions evasion and fraudulent reporting being unveiled again by the US judiciary a few years down the road. Despite whatever differences there were in the respective cases, the DPAs that were signed by all these financial institutions and US judicial authorities remained remarkably similar specifically with the requirements that needed to be met with regard to due-diligence, software requirements and the hiring of independent monitors. The majority of deferred prosecution agreements have stipulations such as 'HSBC Bank USA must implement a new customer risk-rating methodology based on a multifaceted approach that weighs the

---

[26] Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets Control, Section 8-1, December 2004 < www.fdic.gov/regulations/safety/manual/section8-1.pdf > accessed 30 October 2020. See a complete list of resources on US legislation applicable to compliance here <www.sec.gov/about/offices/ocie/amlsourcetool.htm > accessed 30 October 2020.

[27] Financial Action Task Force, 'Recommendations' 16 February 2012 <www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html> accessed 30 October 2020.

[28] Association of Certified Anti-Money Laundering Specialists (ACAMS), 'Navigating FATF Recommendation 16' September 2016 <www.acamstoday.org/navigating-fatf-recommendation-16/ > accessed 4 July 2020.

[29] As one SCB employee wrote, 'this account must remain completely secret to the US' At that time, the CEO of Standard Chartered's Iran representative office wrote a memo in support of expanding the Central Bank of Iran account noting that '[t]o be the bank handling Iran's oil receipts would be very prestigious for SCB. In essence, SCB would be acting as Treasury to the CBI/the country'. See Department of Justice, 'Standard Chartered Deferred Prosecution Agreement' (2012) <www.justice.gov/opa/pr/standard-chartered-bank-agrees-forfeit-227-million-illegal-transactions-iran-sudan-libya-and> accessed 4 July 2020.

following factors: (1) the country where the customer is located, (2) the products and services utilized by the customer, (3) the customer's legal entity structure, and (4) the customer and business type'.[30] The agreements also included provisions regarding the software systems banks use. For instance, BNP Paribas' deferred prosecution agreement states that 'BNP must update its automated monitoring system. The system must monitor every wire transaction that moves through BNP USA. The system must also track the originator, sender and beneficiary of a wire transfer allowing BNP to look at its customer's customer'.[31]

The use of such software packages has become largely unavoidable for any financial institutions seeking to do business within the United States. For the banks that were charged with sanctions busting, such as BNP Paribas, HSBC and Standard Chartered, installing new software packages that monitor every wire transfer that goes through the bank was not just recommended as best practice, but rather, it was included as part of the legal conditions outlined in their deferred prosecution agreements.

Moreover as part of the settlement agreements, the majority of the banks were also placed under the supervision of independent monitors who would file quarterly updates on the bank's progress. The independent monitors come from a private firm approved by the US government, and the banks are forced to pay their fees/labour costs. According to one compliance expert we interviewed,

> Because the DPA says we need to be monitored we pay [our monitors] somewhere in excess of $15 million a year just for their labor costs … I think altogether our compliance costs are fast approach a billion. So that is $1 billion we spent on compliance for financial crime – not even talking about the rest of legal compliance.

The number of independent monitors that are brought in to any given bank can be upwards of 50, and they do not just observe from afar. The monitors move into the respective bank's office space and involve themselves with the inner-workings of the bank's day-to-day operations. As various interviewees with experience working on the floor of a compliance department of a global bank under monitoring programmes told us, the monitors are given total access and at any given moment they can demand to see what an employee is currently working on and how they respond to the software detection signals.

Essentially what this creates is the impression of a panopticon situation where everyone working in the compliance department feels as though they are constantly under surveillance through the adoption of new software technologies that make the possibility of sanctions-busting and non-reporting fraud harder to perform. Indeed, these sanctions busting cases, and the DPAs that were ultimately signed, emphasize the role of technology and monitoring software that underpins a banks' compliance department. However, whether this impression of control is translated in practice into increased efficiency remains an open question. As Umberto Eco writes about the process of digitalization, which is made possible by the increasing amount of publicly available information on the world wide web – in which Eco sees 'the mother of all lists' – and the increasing reliance of algorithms analysing such information, the digital world has become 'both web and labyrinth' which 'really does offer us

---

[30] Department of Justice, 'HSBC Deferred Prosecution Agreement' (2012) <www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations>.

[31] OFAC (n 25).

a catalogue of information that makes us feel wealthy and omnipotent, the only snag being that we do not know which of its elements refers to data from the real world and which does not'.[32] The turn to digitalization in the world of compliance may give the impression to the regulator that banks can effectively monitor a mass of information like that processed daily by banks operating millions of financial transactions, but it may be a misleading impression. But as will be discussed, the relationship between the practical world of compliance in banking and the theoretical logic of how the digital world is supposed to be regulated through and by software is a messy one, in which the human factor figures prominently.

3. THE LIMITS OF ALGORITHMIC GOVERNANCE: DELIMITING THE SOCIAL SPACE OF THE HUMAN FACTOR

It is necessary to move from the world of regulators, lawyers and negotiators of DPAs, to the world of the back office where decisions are translated into routines and practices in order to understand how US regulatory obligations – or rather, new interpretations of what global banks need to do in order to be able to demonstrate regulatory compliance with US law – have been translated in practice by global banks that signed their DPAs with the DoJ in the 2010s. As Bill Maurer writes in an early article on compliance, 'in the last fifteen years or so, numbers of compliance officers have expanded exponentially'.[33] As global banks have been attacked on all sides since 2008, either for their predatory credit practices leading up to the sub-prime crisis or for their gross lack of concern for the regulations and laws imposed by sovereign governments regarding AML legislation or specific sanctions against countries accused of representing a risk to international security (like Iran or the DPRK), the recruitment of 'ethical' or 'care' officers in the otherwise masculine world of care-free banking seemed logical. This growth may have reflected the industry's organic response to a problem inherent in its globalized working, but as we have demonstrated, it was also imposed by the US government in the DPAs that the DoJ has signed with global banks.

Still, concerns for transparency, traceability and the fight against illicit finance in which most compliance officers serve as front-line soldiers, were not non-existent prior to the 2000s and the wave of DPA signings of the 2010s. But before 9/11 and the diffusion of the risk-based approach favoured by regulators, banking technologies were quite crude, and suspicious transactions, withdrawals and transfers were mostly identified through personal contacts rather than the automated software programs that are now used by banks to check the identity of their customers against lists produced by regulators and widely diffused by states and international organizations, especially the United Nations – rather than lists produced by the banks themselves. It is only since 9/11 and the rise of CFT that banks have received digital updates of lists of suspects on a daily basis.[34] With the growth of the compliance industry, lists have gone from being primarily an internally-produced relationship management tool to identify high-net

---

[32] Marieke de Goede, Anna Leander and Gavin Sullivan, 'Introduction: The Politics of the List' (2016) 34(1) Environment and Planning D: Society and Space 3–13, 8.

[33] Maurer (n 15) 483.

[34] World Check, 'Refinitiv World-Check Risk Intelligence' 2020. <www.refinitiv.com/en/products/world-check-kyc-screening> accessed 4 July 2020.

worth clients and to determine which customers should be receiving specific marketing and promotional offers, to externally-produced items screened by software designed to track and flag suspicious financial behaviour among their customers. According to one expert,

> When it came to name recognition software, it didn't exist. Banks had nothing – nothing at all to check their records and Citibank was the very first bank that had a program and they wrote the program themselves and [this one person] who used to work at OFAC and then became a compliance officer for Citibank … said oh, we'll show you literally where – where the software is, we can literally physically go there to see it. And there was not a single bank in Europe in 2000 that was using any kind of name recognition software. So this whole industry did not exist [before] … September 11 and then it becomes a competitive market, now you can receive email updates, changes on the UN list, the EU list, OFAC – It's now a very lucrative business and again – it's a lucrative business because people are in the market for products which they think can offer up a solution.

Banks now routinely screen their customers against public and private terrorist watch-lists, sanctions lists, geographical areas (that is, the Middle East and Africa), and finally, what makes sense in terms of the financial behaviour of a customer.[35] Progress in the management of such external lists was key to helping banks become more efficient. For example, one of the tools most commonly used by financial institutions around the World is a screening software program called World Check. World Check screens a financial institution's entire client list against global sanctions lists (US, UN, EU, UK, etc.), lists of Politically Exposed Persons, Narrative Sanctions Lists, Global Regulatory and Law Enforcement Lists, Iran Economic Interest (IEI) and others. Screening is done whenever a new customer (individual for retail purposes or a corporate institution) is onboarded, and the entire client population is screened at least once a week so as to make sure any changes on global sanctions lists are captured.

The compliance officers we interviewed found that the growth of the financial intelligence industry has helped improve the system of global surveillance of digital money flows, which helps them perform their duty of care and due diligence. But in fact, our interviewees often also look at the adoption of new software technologies critically, as only constituting a legal response to the increased regulatory scrutiny of the US government after a number of these same global banks were caught not complying with US sanctions when operating transactions through US territory. In order to understand how certain banks use banking technology software and how compliance officers understand their merits or limitations, we must first understand what this technology is and how it operates. As said, for years now, banks have utilized technology for datamining purposes in order to create profiles of their customers to determine their profitability and target which promotions should be sent to which clients. Because of this, banks and the financial sector have mountains of information on their clients as well as on their businesses and personal finances. But without an algorithm to read through these constantly updated lists of terrorists, sanctions-busters or politically exposed persons, a bank may find the amount of data to be dealt with is too much for a human to handle, which is why they need to develop some automated way of processing the information. As Fleur Johns writes,

---

[35] Sullivan (n 11).

> The algorithm enjoys no natural or necessary association with the list, yet the two are frequently related: the algorithm feeds and cleanses the list; it is the list's carer. It is the background to the list's foreground; the engineering to its interface; the murmur to its shout.[36]

A number of incredibly sophisticated software technologies exist that are supposed to help compliance officers avoid freezing the assets of the innocent and determine with a high degree of certainty if a match exists between listed individuals and some of their clients whose assets they are legally required to freeze. The alternative to Googled information is indeed for the bank to either buy or to develop software that will do the job of data selection and triage, which will allow the human compliance officer to concentrate on the task of analysing whether the information looks pertinent and actionable or whether it is lacking. Some financial institutions have developed their own software for datamining, but more often than not, they rely on software packages developed by outside vendors such as NetEconomy, Norkom, World-Check, ATTIV/O, and QuantaVerse. The use of such software packages has not only become unavoidable for financial institutions, but in some cases, banks are actively seeking out partnerships with technology companies. For example, HSBC has developed an advisory board composed of various CEOs and technology scientists working in Silicon Valley to provide it with guidance on technology and digital strategies.[37]

This is no easy task, as there is not one central database to screen for all potentially suspicious individuals, locations or transactions.[38] Instead, software programs have to be manually set to screen against public and private terrorist watch-lists, other sanctions lists, and geographical areas and territories that have been deemed 'high-risk' (that is, the Middle East, Africa and the majority of the Caribbean). In other words, despite the fact that these software systems are technically designed to track and flag anything suspicious, it is the employees at the bank who are responsible for writing the rules, or codes, that determine what the software programs will flag as suspicious. And checking for blacklisted names is not as straightforward as it may sound. Not only are banks required to check against several national lists – including, for example the US (OFAC SDN List & Bureau of Industry and Security (BIS) List of Denied Persons), UK, EU, Israeli and UNSC lists – but they are also required to check against privately compiled politically exposed persons (PEP) lists, which include individuals who, because of their political roles, may be increasingly vulnerable to corruption.

Here, in many ways, the issue of extraterritorial implementation of US, EU or Israeli law is merely a technical question determined by the choice of the compliance office to set the right parameters in the software: either by restricting the names on each national sanctions list to the relevant territories where such national authorities have jurisdiction (first case); or by adding all names in a global dataset of designated entities, enabling the global banks to be on the safe

---

[36] Fleur Johns, 'Global Governance Through the Pairing of List and Algorithm' (2016) 34(1) Environment and Planning D: Society and Space 126–49, 127.

[37] Tanaya Macheel, 'HSBC Turns to Tech Execs for Guidance' (2017) American Banker <www.americanbanker.com/news/hsbc-turns-to-tech-execs-for-guidance>.

[38] It is also important to differentiate between name screening and payment screening. Name screening is the process of matching an internal record (client, counterparty, etc.) against a sanctioned list record. It is generally more feasible to stop a customer's onboarding when list screening flags a possible connection between the potential customer and a sanctions list. Payment screening on the other hand focuses on the screening of payment messages. This particular type of screening takes place with current customers and is performed before a payment or message is processed.

side if these individuals are involved in dollar-denominated or euro-denominated transactions and even if the transactions take place outside the US or Europe (second case). In the first case, sanctions laws remain national in scope, with banks implementing the law of each country only; in the second case, sanctions laws are given 'extraterritorial' effects by global banks. Of course, as banks became increasingly risk-averse after 11 September 2001, leading them to add more names of designated terrorist affiliates and to avoid limiting the implementation of transactions restrictions to national jurisdictions only, they increasingly adopted an extra-territorial approach to sanctions implementation, especially after the Executive Order of 24 September 2001, signed by President Bush, which increased both the number of individuals and organizations named on the US list as well as the ability of US authorities to detect and block transactions associated with individuals on those lists.

There are millions of individuals and entities across the globe listed on these public and private watch-lists, and these lists are updated on a daily basis.[39] Similarities amongst various names, problems transcribing names from one language to another and the fact that these lists are always changing, means that even something that sounds as simple as checking or screening a name is fraught with countless complications. As an interviewee admits:

> The key issues that we commonly identified during that time, and to tell you the truth we still do see them … is that you are screening billions and trillions of transactions monthly and you do get – if you[r] [software parameters] are too sensitive – you get so many hits! So how do you deal with all of them, and what is the right size of the team, what's the level of screening that you have to put in place to be able to then find that needle, right?

The technical difficulties encountered by compliance officers are not always understood by judicial authorities (especially in the US enforcement arm), who may be tempted to believe that all financial crimes could be eradicated if banks were legally obligated to adopt strong software technologies which screen every transaction in search of suspicious patterns. But such a naïve belief ignores the fact that banks are reliant on a whole informational eco-system which they cannot control (and which they often have to pay to get access to) in order to detect suspicious terrorism- or proliferation-related activity. If we take the example of sanctions-busting detection, general guidelines are far too broad to allow any human compliance officer to correctly interpret the information that they are supposed to look for. For instance, the following list details what a global bank's internal sanctions policy asks its employees to look for:

> Business Lines, Jurisdictions, and Employees are responsible for identifying any Client with known exposure to a Sanctioned Country. Any known exposure to a Sanctioned Country should be considered: however, some of the circumstances in which such exposure exists include the following: Client is subject to a Sanctioned Country tax jurisdiction; Client is located in a Sanctioned Country; Client is doing business in or with a Sanctioned Country; Client is owned in whole or in part by a legal entity or an Ultimate Beneficial Owner located in a Sanctioned Country.

As anyone can immediately see, more than half of the globe is concerned by such a policy, which over-extends the notion of 'high-risk territory' to any territory sanctionable by any of the Western states. In this case, does this internal requirement mean for the compliance officer

[39] LexisNexis Risk Solutions, 'Sanctions List Screening' <https://risk.lexisnexis.co.uk/businesses-and-non-profits/financial-crime-compliance/watchlist-screening/sanctions-list-screening> accessed 4 July 2020.

that a client who is Russian (under sanctions from the EU and US) cannot have a bank account in the bank? Would that mean that the bank account of a client who has a business relationship (trade? or even travel?) in a country such as Russia needs to be closed down? In this case, high risk jurisdictions are not just countries that are sanctioned, they can include countries that are 'in close proximity to or have trade ties to a country subject to Comprehensive Sanctions'. This even lengthens the list of sanctioned territories to the limits of absurdity. Would that mean that any client from Poland would have to be under special scrutiny because it is close to Russia, which is under EU sanctions? Of course, such a broad understanding of the bank's internal bylaws would be too discriminatory to become operational. But if internal rules are too broad, then, it is important that banks provide the right amount of detail to the software designers so that the latter do not exclude too many bank accounts or too few.

The notion of high-risk territories is thus a key variable for compliance officers as they set the parameters of the software program their bank is using. This includes but is not limited to countries with a 'reputation' for being tax havens, countries 'supporting' terrorism and countries that are subject to comprehensive sanctions, and it also includes a low volume of USD-denominated cross-border transactions (moderate level of risk) or high level of USD-denominated cross-border transactions (high level of risk). In this case, the bank compliance officers rate the extent to which they are likely to apply US sanctions law to screen a non-US client's transactions based on its exposure to USD-denominated payments (even if these payments are not associated with transactions involving US persons or US territory). This shows how the OFAC ruling of 2008 on the inadmissibility of U-turn transactions in the case of sanctions against Iran, for instance, can become integrated into the daily routines of compliance officers. When they are confronted with such claims as those made by OFAC about the applicability of US sanctions law to all USD-denominated transactions across the globe, even when parties to the transactions are not US persons, and the sale does not cross US territory at any point, compliance officers do not reason whether they should implement it or not based on legal arguments. For them, the argument is merely pragmatic and technical. They have to see whether the software allows them to block such transactions or whether they can set the parameters so that US sanctions can somehow be scaled to the right level of transactions so that they do not apply everywhere. Extraterritoriality of US law is for them mostly a technical rather than a legal problem.

Therefore, when setting the parameters for the monitoring software, it is not enough to simply screen against sanctions lists, banks must also come up with their own internal calculus with regard to how to risk rate countries they or their customers do business in or with. To limit the human arbitrariness in KYC investigations, banks have entire policy documents dedicated to what they refer to as 'Risk Assessment Methodology' as well as 'Client Risk Rating Models'. This relative flexibility in how each global bank sets the parameters of its detection software largely depends on the dialogue (real or fictional) that the bank expects to have with the regulators, as acknowledged by one of our interviewees:

> You can set parameters for how the software is going to operate. So there is a whole theology behind this and there are whole teams of people who do nothing but this. But basically, you want to be able to demonstrate to a regulator that you have thought carefully about how you set your parameters and you want to make sure that you are not excluding possible hits, but at the same time you can't bring everything to a screeching halt … And there are different competing products that promise to boil the ocean a little bit better for you or a little bit faster … and there are some really sophisticated ways of testing your system … but [with something like sanctions] it is just the sanctions blob. And it is all

> types of sanctions, all manifestations of sanctions that banks have to implement … some sanctions programs are more complicated than others so [with] some sanctions programs you could have a hit on an entity, but maybe the activity is permissible or not … or if it is Cuba you can do U-turn transactions you cannot do that with Iran. So every sanctions program comes in different flavors and it is the bank's job to make sure that it is implementing each flavor of sanctions properly.

To a great extent, banks and software companies are left in the dark by the regulators about how they can actually decide how best to fight against money laundering or terrorism/proliferation financing. In order to find the parameters that are best to catch and block suspicious transactions, banks have the capacity to test how the software reacts when they change such parameters. Depending on whether they play with the 'fuzzy logic' or set strict parameters, which will end up eliminating fewer or higher numbers of transactions and lead to the identification of client names, compliance officers can work on a range of variables and run experiments. However, compliance officers, especially those in global banks which are already under a monitoring programme because of the DPA signed with the DoJ, rarely engage in such experiments and instead give precedence to a form of 'non-knowledge'.[40] One of their main fears is that if they set the parameters too broadly, the software will then highlight a long list of new names that regulators will then be in a position to identify. The software is designed in such a way that compliance officers cannot delete the history of their manipulations of parameters, so any name that may pop up during an 'experiment' will be treated by the regulator as a possible suspect, and the regulator will then be in a position to ask bank compliance officers why they did not investigate all the names that appeared, even during 'experimentation'. Experimentations are here 'performative'[41] in the sense that they may produce negative effects. This situation explains why compliance officers are very careful with experimentations: in most instances, the costs of eliminating many names wrongly identified by the software would be way too high to be worth the effort; and, should they not foot these costs, the risk of a high fines decided by the regulator would greatly increase. As software searches are an open book to regulators, compliance officers cannot operate in a fictional space where 'hits' do not matter and names can be erased with the stroke of a pen. This predicament places compliance officers in a position in which they favour non-knowledge over knowledge when it comes to designing the best parameters for their software.

Many compliance officers express criticism of the importance taken on by software management. But they do not do so on principled grounds, like the invasion of privacy and the risks of data misuse that poor data protection mechanisms and centralization of information create for bank customers. Rather they argue the system is ineffective at achieving the goals set by the regulators. One compliance officer summarized the issue with the regulations and the ways in which they constrain banks' ability to master the software in a very critical way. For him, the new three-pronged approach which consists in monitoring, triaging and excluding based on suspicions, and which has worked up steam since 9/11 and the global push in AML, CTF and CPF, is based on mistaken assumptions that only accentuate the risks of driving offenders deeper under cover without setting up real obstacles to their money flows:

> It's just – it's a fruitless exercise. It's almost – I almost feel like [it would be better if we] just didn't have any [regulations] and then all the flows [of money] come so that we can build, invest our time,

---

[40] Mallard and McGoey (n 18).

[41] Douglas Holmes, 'Economy of Words' (2009) 24(3) Cultural Anthropology 381–419.

> energy and money and the technologies to screen the transactions. We [would] divert the funds from the compliance and bullshit governance activities that we do, which we know have very limited impact – and reinvest that into studying data analytics … I almost feel it's actually better to let one of the flows come through because it's with those flows, it is with having access to those flows that you can actually have information to link situations together. We say oh, high-risk countries Sierra Leone, Angola, whatever, we won't take payments from them. Okay that is fine. You cut off your right arm but you know what? There are 54 countries in Africa. They're going to just move it across the border to another country that is considered less risky … Let's say South Africa. Or you know, Cote d'Ivoire, Cameroon those are deemed less risky than Algeria and Tanzania, but there is no border patrol. So they will just move the money across. So it's kind of like really – it does not really help. However, if you remove the restrictions and let them put the money through at least we've got a record of it.

This compliance officer is thus highly critical of the effectiveness of the new legal infrastructure that banks have had to put in place. Not to mention that some software technologies are not secure enough to prevent hackers from disrupting their services, as illustrated by the hacking of the SWIFT software by North Koreans who sent money from the Central Bank of Bangladesh to North Korean accounts. Still, as far as principles do matter, one of the major concerns some compliance officers working in non-US banks have with installing monitoring software is where the data is being held, and whether or not the US government will be able to gain access to their clients' data. Experts have pointed to who exactly owns and controls these software companies from which global banks buy their products, not to mention what happens to the data they collect. As one compliance expert acknowledges:

> Well to be fair, a lot of the software companies… are thinly capitalized Israeli companies. Nobody wants to house their data in a black box that someone else has access to, especially if you are Iran because they do not want to give over control like that to someone else. So there is some structural issues with sanctioned countries re-joining communities because they're naturally paranoid that things could reverse back … connecting these countries, the first thing we would do is infect their banking system with a virus and try to shut them down … we have done it before … the whole notion of cyber warfare cannot really be divorced from banking because it is the major target.

So what is the solution for banks and governments who, like Iran, wish to join the global financial system but are understandably hesitant when seeing how the US government has pulled out of a deal as hard-negotiated as the 2015 Joint Comprehensive Program of Action (JCPOA), which was itself the object of a legally binding UNSC Resolution (UNSCR 2231) under Chapter VII? Many bankers in Iran, for understandable reasons, are unwilling to install and utilize the standard software programs for fear of data breaches and the potential for malware to infect their systems. Some have looked at blockchain, the technology behind cryptocurrencies such as Bitcoin and Ether, as the solution to the concerns surrounding the current software, but even though some of the major global banks are investing in blockchain technology, its use is still in its infancy, especially in the field of trade-finance, which is still heavily reliant on a paper-based system that by its nature is liable to fraud.[42] For example, Bank of America is currently working with Microsoft in order to develop software that utilizes blockchain technology in order to transform the monitoring of trade finance, an area which

[42] PricewaterhouseCoopers, 'Trade Finance: Understanding The Financial Crime Risks' 2016. <www.pwc.co.uk/forensic-services/assets/pwc-and-polestar-financial-crime-risks-and-trade-finance-July-2016.pdf > accessed 4 July 2020.

is still highly manual.[43] Despite these predictions, the software is still reliant upon humans having a clear understanding of what risks the bank is exposed to and setting the software parameters accordingly.

4. CONCLUSION

Banks were not always considered to be the front-line operators in the global war against terrorists or proliferators and their financiers. As one expert in counter-proliferation financing told us, in the 1990s and up to a certain point in the 2000s, the intelligence community put the emphasis on following commodities, by following ships, and by accessing data from private insurance companies like Lloyds or other data companies like Winwood, which use algorithms 'to track when ships switch their automated information systems off and it can monitor hundreds of vessels at the same time and so you can set up parameters and all the imagery appears with Google-type of quality so you can see where in the port they'd be picking up and delivering and if it's coal, you can see it, yeah'. As this expert adds, summing up the general opinion in the field of counter-proliferation finance in the mid-2000s:

> People say follow the money. If you can't follow the money, follow the weapons and if you can't follow the weapons, follow the ships and if you can't, you know, you can follow ships and aircraft and you can follow weapons some of the time. Following the money is the hardest.

Still, after the wave of fines imposed upon global banks accused of sanctions-busting activities in Iran and Sudan in 2013 and 2014, regulators have placed an increasing burden on banks so that they adopt software, which, according to their hopes and dreams, would make it impossible for them to violate regulation ever again. As we have demonstrated, the system is still very much in its infancy and opportunities for human mistakes, deception, and unintended consequences are many. It will then come as no surprise if the US government engages in yet another round of accusations against global banks, who may find themselves accused again of not conforming to the US interpretation of what sanctions-busting in the case of Iran sanctions means. As some of the interviews demonstrate, this new cycle of accusations may then bring about a new cycle of technological innovation, and new spending on the part of banks. As one expert says, banks and financial services only take the regulations seriously when under public or judicial scrutiny. One reason is that their main concern is to make money and to not lose profitable relations by interpreting sanctions obligations too broadly and severing ties with dubious clients; another reason is that some of the compliance specialists find the mammoth legal infrastructure that was created after 9/11 and after the 2013–2014 rounds of sanctions against Iran to be wholly ineffective, if not counter-productive.

In the end, the whole legal infrastructure which grew as a result of this cycle of norm enforcement and rule innovation has fed a new consulting industry, which charges tremendous fees to reluctant banks that do not want to risk another investigation by attacking the new obligations imposed on them by judicial authorities. As one expert said, as compliance

---

[43] Abdel-Qader, Aziz Finance Magnates, 'Microsoft and BofA Team Up to Transform Trade Finance Through Azure Service' 2018. <www.financemagnates.com/cryptocurrency/innovation/microsoft-boa-team-transform-trade-finance-%E2%80%8Eazure-service/> accessed 4 July 2020.

requirements grew exponentially for global banks, new business opportunities emerged, in which 'the big four [global consulting firms] were absolutely favored over the second tier firms just because of the scalability and also because of the fact that these projects were huge and Deloitte has like 180,000 employees and PWC had like 120,000 employees'. As these two professional service organizations make over $25 billion in revenue profit they have largely benefited from global tension over the right approach to compliance, especially in the fields of sanctions or AML, and they are very likely to endorse US sanctions law everywhere, considering their ties to the US financial system. With such economic interest in sustaining the integrity and legitimacy of the new compliance infrastructure that banks have had to implement to align themselves with US sanctions law, it is unlikely that internal criticism voiced in the privacy of compliance floors will be turned into a public challenge against its operations in the near future. In this broad socio-technical context, US sanctions are likely to continue to have extraterritorial effects for a long time.

NOTE