Volume **5** (2) 2023 https://doi.org/10.5204/lthj.2506

Automating Sanctions Compliance: Aligning Regulatory Technology, Rules and Goals

Oliver Hackney
Australia
Anna Huggins
Queensland University of Technology, Australia

Abstract

The raft of sanctions introduced by governments throughout the world in response to the Russia-Ukraine conflict and other situations of international concern underscores the complex and rapidly changing nature of sanctions regulatory expectations. This article critically examines the extent of alignment between regulatory technology (RegTech) and sanctions compliance requirements, using the nascent Australian sanctions regime as an illustrative example. Applying insights from regulatory theory, the article differentiates between regulatory rules and goals to facilitate a nuanced evaluation of the prospects of automating sanctions compliance. It also analyses the potential disconnects between RegTech and sanctions rules arising from flaws in an automated system's design, data inputs or underlying code, and mismatches between the capabilities of RegTech and the overarching regulatory goal of promoting a culture of compliance. The article argues that ongoing human interaction with well-calibrated RegTech tools is needed to promote alignment between RegTech and regulatory rules, and to meaningfully contribute to the broader culture of compliance goals. These insights have transferable relevance to diverse jurisdictions with complex sanctions compliance requirements and to other regulatory domains.

Keywords: Sanctions regulation; compliance; RegTech; automation.

1. Introduction

The raft of sanctions introduced by governments throughout the world in response to the Russia-Ukraine conflict and other situations of international concern underscore the importance of compliance with sanctions regulations. In the Australian regulatory context, for example, the Federal Government has adopted a broad sanctions package in response to the Russia-Ukraine conflict, including targeted financial sanctions and travel bans against Russian military personnel, oligarchs, key government officials, members of the Russian Security Council, key financial institutions, pro-Kremlin propagandists, Belarusian military and government personnel, and organisations involved in the supply of weaponry to Russia or surveillance technology used to persecute protestors.[1] These sanctions sit alongside 23 other active sanctions regimes the Australian Government has imposed in response to situations of international concern.[2] This recent spate of activity highlights the expanding sanctions regulatory requirements and the need for organisations to adapt their compliance approaches to satisfy the evolving legal requirements.

The authors gratefully acknowledge the helpful comments of the anonymous reviewers and the funding received from the Human Technology Law Centre at Queensland University of Technology.

[1] See *Autonomous Sanctions Amendment (Russia) Regulations 2022* (Cth); *Autonomous Sanctions Amendment (Ukraine Regions) Regulations 2022* (Cth); *Autonomous Sanctions (Designated Persons and Entities and Declared Persons—Russia and Ukraine) List 2014* (Cth); *Autonomous Sanctions (Import Sanctioned Goods—Russia) Designation 2022* (Cth); *Autonomous Sanctions (Export Sanctioned Goods—Russia) Designation 2022* (Cth). The Russian Government has also imposed sanctions on Australian military personnel, journalists, academics and business officials accused of furthering Australia's 'anti-Russia policy line': Ministry of Foreign Affairs of the Russian Federation, "Foreign Ministry Statement."

[2] Department of Foreign Affairs and Trade, "Australia and Sanctions."

Except where otherwise noted, content in this journal is licensed under a Creative Commons Attribution 4.0 International Licence. As an open access journal, articles are free to use with proper attribution. ISSN: 2652-4074 (Online)

© The Author/s 2023

The highly charged and rapidly changing sanctions regulatory context raises important questions about the extent to which regulatory technology (RegTech)[3] can be appropriately deployed to fully or partially automate sanctions compliance processes. The most common type of RegTech employed in sanctions compliance programs is known as 'sanctions screening technology'.[4] This technology uses screening software to detect, prevent and disrupt sanctions risks, and compare data uploaded by users against lists of sanctioned parties.[5] For example, sanctions screening technology can employ a name-matching algorithm to compare the name of an individual or entity that a user uploads to the names included in sanctions lists that are made publicly available by governments. This highlights a unique opportunity for automated decision making (ADM) in the sanctions context, as the regulation requires organisations to compare two sets of data to detect a sanctioned party: that is, the list of sanctioned parties and the users' data. *Prima facie*, this data comparison task is well suited to automation as opposed to broader subjective or value-laden regulatory decisions.[6] However, the potential applications of RegTech are by no means limited to sanctions screening or indeed sanctions compliance. A deeper understanding of the benefits and limits of automated compliance processes is likely to be of interest to diverse regulated industries, especially as RegTech is expected to become a $55.28 billion industry by 2025.[7]

RegTech solutions offer organisations an opportunity to enhance the efficiency, accuracy and cost effectiveness of their compliance processes. However, there is a risk that the adoption of RegTech may be mere 'window dressing' or a symbol of a commitment to compliance without properly integrating the use of RegTech into day-to-day regulatory compliance practices.[8] In other contexts, the problem of the disconnection between the law and technology is recognised as being 'both acute and chronic'.[9] However, the extent of the disconnection between RegTech and sanctions compliance remains underexplored. This article addresses this lacuna by analysing a range of potential disconnects in the context of sanctions RegTech and opportunities for narrowing these gaps. To facilitate a nuanced evaluation, the article draws upon the regulatory theory distinction between compliance with regulatory rules and compliance with collective regulatory goals.[10] It shows that disconnects between RegTech and regulatory rules can arise from flaws in an automated system's design, data inputs or underlying code. There are also mismatches between the capabilities of RegTech and broader human-centric regulatory goals of promoting a culture of sanctions compliance.[11] The article argues that these disconnects need to be acknowledged and addressed by ensuring ongoing human interactions with well-calibrated RegTech solutions. The insights yielded from this analysis in the Australian sanctions compliance context have transferable relevance to diverse jurisdictions, notwithstanding the differences in the specific regulatory rules and goals that apply in each context.

The article proceeds in four sections. Section 2 further contextualises the importance of sanctions compliance and the nascent Australian regulatory framework. Section 3 outlines different conceptualisations of RegTech and the types of automated tools that are most commonly used for sanctions compliance purposes. Section 4.1 differentiates between compliance with regulatory rules and goals as a basis for analysing the extent of the disconnect between RegTech and regulatory compliance expectations. Section 4.2 analyses a range of disconnects arising from deploying RegTech tools to automate compliance with regulatory rules. As the Australian sanctions regulatory framework is still in its infancy, this sub-section incorporates lessons learned from the deployment of RegTech solutions in the United States (US) sanctions compliance context. Section 4.3 examines the extent of the alignment between sanctions RegTech and the regulatory goal of the Australian sanctions regime: namely, promoting a 'culture of compliance' with sanctions requirements.[12] Section 5 argues that human oversight of and interaction with well-designed sanctions RegTech is needed to address the disconnection between the capabilities of RegTech and the holistic requirements of a robust compliance regime.

[3] 'RegTech' can be defined as the use of digital and automated technologies to facilitate regulatory monitoring, reporting and compliance: Arner, "FinTech, RegTech, and the Reconceptualization," 374. However, as is discussed further in Section 3, definitions of RegTech are diverse and contested.
[4] Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening," 1.
[5] Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening," 2.
[6] For further discussion on automating discretionary requirements requiring the weighing of different factors and values, see Perry, "iDecide."
[7] Grand View Research, "RegTech Market Size."
[8] For an analysis of this issue beyond RegTech, see Parker, "Internal Corporate Compliance Management Systems," 171.
[9] See, e.g., Brownsword, "The Challenge of Regulatory Connection." See also Bennett Moses, "How to Think about Law," 1, 7, 19 and Huggins, "Addressing Disconnection."
[10] Yeung, Securing Compliance, 11. See also Parker, "Reinventing Regulation within the Corporation," 529–565. See also Section 4.1.
[11] Replacement Explanatory Memorandum, Autonomous Sanctions Bill 2010, 2. See also Section 4.3.
[12] Replacement Explanatory Memorandum, Autonomous Sanctions Bill 2010, 2.

2. The Regulatory Framework for Sanctions Compliance

To provide context for this analysis of automating sanctions compliance, this section first outlines the background, purpose and complexity of the Australian legal framework underpinning the sanctions regime. The regulation of sanctions in Australia has been gaining prominence in recent years. In December 2021, the Federal Government introduced new legislation establishing thematic sanctions regimes in areas such as human rights, cyber security and weapons of mass destruction, capturing entities and individuals outside sanctioned countries and adding a further layer of complexity to sanctions compliance obligations.[13] These changes are in addition to establishing a dedicated sanctions regulator, the Australian Sanctions Office (ASO), in 2020. The creation of the ASO arguably signals an intention to align the Australian approach to enforcing sanctions laws with other dedicated sanctions regulators in the US and the United Kingdom,[14] both of which have imposed significant financial penalties in response to violations of sanctions law.[15] This complex and rapidly changing compliance environment underscores the importance of sanctions compliance considerations within Australian organisations, particularly for those with an international presence.

There are two main components of the Australian sanctions regime: (i) United Nations Security Council (UNSC) sanctions, which Australia is bound to implement as a United Nations (UN) member state;[16] and (ii) Australian autonomous sanctions,[17] which are executed by the Australian Government independently and not pursuant to any international obligation.[18] Similarly to the autonomous sanctions of many other jurisdictions globally,[19] both the UN and autonomous sanctions carry an extraterritorial effect if there is a sufficient geographical connection to Australia.[20] The sanctions regimes from multiple jurisdictions may apply to an Australian organisation depending on their business operations; however, this article principally focuses on sanctions under Australian law.

Australia can adopt diverse types of sanctions measures in response to situations of international concern, such as travel bans, asset freezes and export controls, that trigger compliance obligations for organisations.[21] Financial sanctions carry onerous compliance obligations, which restrict the ways in which organisations can legally deal or engage with particular entities and individuals in certain ways. There is no codified definition of financial sanctions in international law or any domestic legal instrument. However, generally, in the international community, financial sanctions refer to measures of an economic character applied to generate the political changes desired by the senders to express disapproval of acts or to induce the target to change its policy, practices or government structure.[22]

The Australian Government commonly imposes targeted sanctions on entities, individuals and groups that require organisations to continuously monitor new additions to sanctions lists and take steps to identify newly designated parties across their operations.[23] Financial sanctions can designate an entire country, known as comprehensive or blanket sanctions, or specific entities and individuals responsible for the situation of international concern, known as targeted or smart sanctions.[24] Due to the unintended consequences of blanket sanctions suffered by civilian populations living within a designated country,[25] the international community has shifted away from blanket sanctions towards a more targeted approach. Targeted sanctions pinpoint specifically identifiable non-state actors responsible for acts of international concern, such as individuals, corporations and groups, which are published in publicly available lists, known as sanctions lists, by governments.[26] This presents a significant challenge to organisations from a compliance perspective, as they must adopt measures to identify designated parties across their operations and accurately monitor the changes to sanctions lists to avoid committing a criminal offence.[27] In

[13] *Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021* (Cth); *Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Regulations 2021* (Cth).
[14] See generally Kerrigan, "Sanctions Regime."
[15] OFAC, the US Sanctions Regulator, notes that total enforcement actions in 2019 comprised nearly $1.3 billion (USD): United Sates Department of the Treasury, "2019 Enforcement Information." For an example of an enforcement action by the Office of Foreign Sanctions Implementation in the United Kingdom with a GBP20.4 million settlement in 2020, see HM Treasury, "Enforcement of Financial Sanctions."
[16] *Charter of the United Nations Act 1945* (Cth) s 6.
[17] See *Autonomous Sanctions Act 2011* (Cth); *Autonomous Sanctions Regulations 2011* (Cth).
[18] Tully, "Implementing Targeted Sanctions," 119; Wyld, "Sanctions 2021," 28.
[19] Wyld, "Sanctions 2021," 28.
[20] *Charter of the United Nations Act 1945* (Cth) s 7; *Autonomous Sanctions Act 2011* (Cth) s 11.
[21] *Autonomous Sanctions Act 2011* (Cth) s 10(1); Ruys, "Sanctions, Retorsions and Countermeasures," 2.
[22] Illieva, "Economic Sanctions in International Law," 201–203.
[23] Tully, "Implementing Targeted Sanctions in Australia," 116.
[24] Portela, "National Implementation," 15–20; Drezner, "How Smart are Smart Sanctions?," 107–108.
[25] Tully, "Implementing Targeted Sanctions in Australia," 116.
[26] See Department of Foreign Affairs and Trade, "Australia and Sanctions."
[27] Tully, "Australia's Autonomous Sanctions Regime," 157–158.

Australia, a body corporate commits an offence where it cannot prove on the balance of probabilities that it took reasonable precautions and exercised due diligence to prevent a breach of a sanctions law.[28]

The complex scope and rapidly changing nature of sanctions regulations pose a significant obstacle for organisations seeking to comply with sanctions legal requirements.[29] The Australian response to the Russia-Ukraine conflict provides an example of daily changes to regulations. On 25 February 2022, Australia imposed targeted sanctions on 339 members of Duma; on 26 February 2022, Australia imposed further sanctions targeting key members of the Belarusian political or military figures and contributing organisations; and on 27 February 2022, Australia designated a number of leading political figures in Russia.[30] These frequent changes create a considerable challenge for organisations seeking to implement compliance programmes that are capable of rapidly responding to evolving sanctions expectations.

The use of digital technology provides an appealing and increasingly popular solution to address the growing volume and complexity of sanctions requirements that apply to business operations.[31] As the Australian sanctions regulatory framework is in a nascent stage, lessons learned from RegTech deployment in other sanctions compliance contexts can valuably inform this analysis. Enforcement actions in the US sanctions context provide useful insights in this regard. The Office of Foreign Asset Control (OFAC) is a longstanding sanctions regulator that was founded in 1950, as opposed to the ASO, which was founded in 2020. The OFAC directly pursues enforcement actions and imposes penalties. Conversely, the ASO plays a role in enforcing sanctions law by collaborating with federal agencies, but it is the Commonwealth Director of Public Prosecutions that brings actions for breaches of sanctions law to court.[32] Since the introduction of the current Australian sanctions regulatory framework, the Australian courts have enforced sanctions law against individuals; however, to date, there has been very little corporate enforcement of sanctions laws.[33] In contrast, OFAC levied $1.3 billion in monetary penalties and settlements across 30 enforcement actions for sanctions violations in 2019 alone.[34] Notably, the third-party providers of sanctions screening technology primarily cater to a global market. Thus, the types of technology used by US corporations are likely to be very similar or the same as the technology procured by Australian organisations.[35] As a result, the legal issues that relate to the use of sanctions RegTech in the US provide valuable insights for Australian organisations implementing similar digital solutions.[36]

3. Managing Regulatory Burden through Sanctions RegTech

Despite the growing traction of RegTech as a business solution, the scope of the RegTech concept remains contested and definitions differ widely.[37] This section clarifies what is meant by RegTech in the sanctions compliance context and analyses its appeal as a compliance solution to address increasing regulatory burden and complexity. Although the RegTech moniker encapsulates a range of digital technologies, the most commonly used technological tools for sanctions compliance are ADM systems for sanctions screening purposes. This section outlines the ways in which RegTech solutions aim to increase the efficiency, accuracy and cost effectiveness of compliance with sanctions regulatory requirements. However, as discussed further in Section 4, these ambitions will be undermined by unsophisticated approaches to digitalisation and misalignments between RegTech and regulatory compliance expectations.

The concept of RegTech has its roots in the financial services industry,[38] but its application is by no means limited to this context. Some definitions treat RegTech as a subset of financial technology (FinTech),[39] which generally refers to the use of technology in financial services solutions.[40] However, the conceptualisation of RegTech as a subset of FinTech fails to consider the use of RegTech in other highly regulated industries with complex regulatory requirements, such as healthcare, charities,

[28] *Autonomous Sanctions Act 2011* (Cth) s 16(7).
[29] For further discussion of the potential for inconsistently applied sanctions laws, see Tully, "Australia's Autonomous Sanctions Regime," 163–165. See also C6 Intelligence, "Technology and Data Analysis," 13.
[30] *Autonomous Sanctions (Designated Persons and Entities and Declared Persons—Russia and Ukraine) List 2014* (Cth).
[31] This phenomenon is evident across diverse regulated sectors. See: Boston Consulting Group and RegTech Association, "Australia's Global RegTech Hub Poised for Growth."
[32] Wyld, "Sanctions 2021," 28.
[33] See, e.g., *R v Choi (No 10)* [2021] NSWSC 891; *R v AA (No 3)* [2019] NSWSC 1982. For details on enforcement concerning conduct that occurred between 1999 and 2003 before the current sanctions framework came into force, see *ASIC v Flugge & Geary* [2016] VSC 779.
[34] United States Department of the Treasury, "2019 Enforcement Information."
[35] See Market Research Store, "Sanctions Screening Software."
[36] See also Section 4.2.
[37] Weber, "RegTech," 11; Arner, "FinTech, RegTech, and the Reconceptualization," 381; Waye, "RegTech," 363.
[38] Johansson, "RegTech," 72.
[39] Anagnostopoulos, "FinTech and RegTech," 120; Wang, "The Role of Regtech," 4.
[40] Arner, "FinTech, RegTech, and the Reconceptualization," 377–378.

policing, supply chains, forestry management and other industries subject to sanctions regulation.[41] Given the potential applications of RegTech across diverse industry sectors, this article argues that it is preferable to conceive of RegTech as an independent phenomenon separate from FinTech.[42] It is also worth distinguishing between Supervisory Technology (SupTech), which refers to the use of RegTech by a regulator, and RegTech tools deployed by regulated entities.[43] This article primarily focuses on the latter. However, it is notable that the Australian Securities and Investment Commission (ASIC) encourages regulated businesses to implement RegTech and has trialled the adoption of SupTech to detect regulatory breaches.[44] There is thus a potential overlap between RegTech and SupTech tools.

Some definitions of RegTech broadly encapsulate the use of diverse technologies to support regulatory activities. One of the earliest definitions of RegTech, provided by the Institute of International Finance (IIF) in 2016, defined RegTech as 'the use of new technology to solve regulatory and compliance requirements more effectively and efficiently'.[45] The 'new' technologies that typically fall under the RegTech umbrella include cloud-based computing, artificial intelligence, blockchain, natural language processing, big data analytics, robotics, distributed ledger technology, application program interfaces and biometrics.[46] In a similar vein, Singh et al. defined RegTech as encompassing all the data and technology used in all parts of a compliance program, including for reporting, risk mitigation and staff training.[47] The advantages of such broad definitions are that they potentially apply to diverse industry sectors and can encompass new generation RegTech tools.[48] However, these broad definitions use such expansive language that they capture compliance with a multitude of non-legal business requirements in addition to binding regulatory requirements. Non-legal applications, such as compliance training tools or business intelligence, may form part of the wider compliance landscape within an organisation. However, these tools have a limited connection to regulatory instruments and are likely to be of little interest to regulators. For present purposes, this article focuses on RegTech tools that have a clear nexus to sanctions compliance requirements in regulatory instruments and tools that facilitate the monitoring and reporting of legal requirements.[49]

In the context of sanctions compliance, the most common RegTech solutions are ADM tools rather than the broad panoply of digital compliance tools listed by the IIF. Sanctions screening technology typically adopts ADM tools to screen user data against the relevant lists and decide whether there is a true match between the user data and the sanctions list, which generally involves minimal human analysis.[50] Sanctions screening technology also offers a raft of other benefits to regulated entities, such as the consolidation of sanctions data from multiple sources into one interface[51] and access to digital portfolios on sanctioned entities containing information on their ownership structures.[52]

The types of ADM used in sanctions RegTech solutions can be classified into two broad categories: rules-based algorithms, and machine-learning or probabilistic algorithms.[53] Rules-based algorithms refer to computational algorithms containing binary, deterministic logic with 'if-then' coding statements.[54] They involve a top-down approach to computation whereby human programmers must amend the coding rules ahead of time to change their functionality.[55] An example of a rules-based algorithm in the sanctions context is as follows: *if* the date of birth for an individual in their user data set does not match the date of birth of a designated individual in the consolidated sanctions list with the same name, *then* consider the hit a false positive. This concentrates staff capacity on the potential hits that have a high degree of similarity to those on the sanctions lists.

Conversely, machine learning refers to algorithms that 'self-learn' from concepts and patterns that the algorithms detect in data sets without predetermined instructions from humans.[56] Thus, machine-learning algorithms can adapt to changing

[41] Wang, "The Role of Regtech," 4; Waye, "RegTech," 365; Weber, "RegTech," 11.
[42] Arner, "FinTech and RegTech in a Nutshell," 10.
[43] Zeranki, "Digitalisation of Financial Supervision," 313.
[44] Australian Securities and Investment Commission, "ASIC's Innovation Hub" 18–19 [72]; Waye, "RegTech," 366.
[45] Silverberg, "RegTech in Financial Services," 2; Wang, "The Role of Regtech," 13.
[46] Wang, "The Role of Regtech," 13.
[47] Singh, "Can Artificial Intelligence," 13.
[48] Arner, "FinTech, RegTech, and the Reconceptualization," 381–382; Weber, "RegTech," 11.
[49] See, e.g., Singh, "Can Artificial Intelligence," 13; Packin, "RegTech, Compliance," 207–208; Clark, "The Opportunities Afforded by RegTech."
[50] Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening," 2.
[51] Johnson, "The Evolution of Sanctions."
[52] Dow Jones Risk and Compliance, "Leveraging Data and Technology."
[53] Surden, "Artificial Intelligence and Law," 1310.
[54] Hildebrandt, "Algorithmic Regulation," 1.
[55] Surden, "Artificial Intelligence and Law," 1317.
[56] Bathaee, "The Artificial Intelligence Black Box," 900.

circumstances detected in the data and produce dynamic solutions given a broad range of factors, while rules-based algorithms produce a static output and have no discretion to consider other computational information outside their coding parameters.[57] Examples of the deployment of machine learning in sanctions compliance include the use of fuzzy-logic algorithms that detect close name variations, the continuous screening of customer data against updates to sanctions lists in real time and extracting patterns from previous decisions made by compliance professionals to minimise the volume of false-positive hits.[58]

A key benefit of RegTech for organisations is its ability to significantly increase the efficiency of detecting sanctioned parties. The features of sanctions screening technology offer organisations an opportunity to reduce the volume of decisions requiring human review and assess potential hits at a pace that is unattainable by human reviewers. This creates an attractive cost-saving business case for implementing RegTech.[59] Moreover, the technology employs a network of algorithms that considers a range of different data points to detect sanctioned entities, screening against metadata from the sanctions lists, which includes their dates of birth, alias, country of birth, country of registration and other identifying details.[60] This further increases the efficiency of reviewing potential hits by decreasing the number of false-positive results that require human review and conserving human analysis for particularly complex potential hits.

In addition to its efficiency advantages, sanctions screening technology offers organisations an opportunity to enhance their compliance with legal requirements. The ability to autonomously screen data against updates to sanctions lists in real time enables organisations to stay abreast of changes to sanctions lists by using RegTech to alert them to instances in which newly designated parties may trigger their compliance obligations.[61] The system capabilities also offer greater access to information about sanctioned parties that would not be visible by manual review, enabling organisations to gain intelligence, which can also assist organisations to determine the appropriate action to take in the event of a positive hit. This greater pool of information can also highlight entities that contain sanctioned individuals within their ownership and control structures, allowing organisations to assess sanctions risks across their operations and to make risk-based decisions about continued engagement with certain unlisted entities with high sanctions risks.[62] Fuzzy-logic algorithms enable organisations to detect close name variations, such as different variations in the name 'Mohammad', which may help organisations to identify sanctioned individuals or entities that adopt different name variations to circumvent sanctions regulations.[63] Thus, sanctions screening technology presents opportunities to significantly improve the efficiency of detecting sanctioned parties and promote compliance with sanctions regulations.

4. Regulatory Technology, Rules and Goals

Although RegTech solutions have the potential to enhance sanctions compliance, disconnects between automated tools and regulatory requirements can create significant legal and regulatory risks for regulated entities.[64] It is thus critical that RegTech solutions are well-calibrated to align with regulatory compliance requirements. Adopting insights from regulatory theory, Sub-Section 4.1 argues that distinguishing between regulatory rules and goals facilitates a nuanced evaluation of the potential disconnects between RegTech and sanctions compliance expectations. Sub-Sections 4.2 and 4.3 analyse the range of potential disconnects that can impede alignment between RegTech solutions and regulatory rules and goals, respectively.

4.1 Compliance with Regulatory Rules and Goals

As the preceding section shows, the majority of RegTech applications predominantly focus on technical solutions for addressing specific regulatory requirements. However, this article argues that a focus on compliance with discrete regulatory standards is necessary but not sufficient for evaluating the extent to which RegTech solutions align with regulatory compliance requirements. As Yeung notes, regulatory scholars sometimes refer to compliance with regulatory standards and compliance with collective goals interchangeably and inconsistently.[65] The two may partially overlap, but they also diverge in important respects. They are not necessarily coextensive, as is demonstrated by the well-known phenomenon of 'creative compliance' in which organisations comply with the technicalities but not the spirit and purpose of legal rules.[66] Accordingly, regulatory

[57] Huggins, "Addressing Disconnection," 1061.
[58] Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening," 11.
[59] See White & Case, "The Emergence," 4–5.
[60] See generally Dow Jones Risk and Compliance, "Leveraging Data and Technology," 8.
[61] See generally Johnson, "The Evolution of Sanctions."
[62] Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening," 7.
[63] Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening," 12. See also C6 Intelligence, "Technology and Data Analysis," 13.
[64] Bamberger, "Technologies of Compliance," 669–739.
[65] Yeung, "Securing Compliance," 11.
[66] Yeung, "Securing Compliance," 11.

theorists emphasise the importance of achieving substantive compliance with regulatory goals alongside technical rule compliance.[67] This article contends that a focus on both regulatory rules and goals is desirable in evaluating the extent to which RegTech is fit for regulatory purposes.

From a methodological perspective, compliance can be valuably illuminated by both a legal and empirical analysis.[68] The analysis in this section adopts the former approach. In relation to rule compliance, this article analyses examples of relevant US enforcement actions that illuminate potential disconnects between the use of RegTech tools and the achievement of compliance with legal rules. In terms of operationalising substantive compliance, Parker and Nielsen outline three key methodological approaches in which compliance is analysed by reference to (i) attitudes and motivations, (ii) policy goals, and (iii) compliance behaviour.[69] This article adopts the second of these approaches, using the government's policy goal in adopting sanctions compliance legislation[70] as a normative benchmark for the analysis in Section 4.2. Although this article adopts a legal analytical approach to evaluate the role of RegTech in promoting compliance with regulatory goals, it is acknowledged that future empirical research on the interaction between RegTech and human compliance behaviour would further enrich this analysis.[71] The following two sub-sections analyse the potential disconnects between RegTech and regulatory rules and goals, respectively, in the Australian sanctions regulatory context.

4.2 Disconnects between RegTech and Regulatory Rules

RegTech solutions can be disconnected from regulatory rules as a result of coding errors, incomplete data sets, the digital mistranslation of regulatory requirements and biases in the code and data. These risks are exemplified by a spate of recent sanctions enforcement actions in the US involving flawed RegTech systems. These examples highlight a range of potential technical and legal disconnects between RegTech solutions and sanctions compliance expectations.

The use of sanctions screening technology by regulated entities in their compliance program does not preclude the possibility of their committing a sanctions offence. As discussed further below, in a number of decisions, OFAC has cited computer system behaviour as a reason that a sanctioned entity went undetected by a regulated entity. In many cases, sanctions screening technology has failed to alert an organisation where a name in their internal data was a close name variation of a designated party, resulting in a sanctions law violation. For example, Cobham Holdings Inc. (Cobham) used third-party sanctions screening software that applied an all-word-match criterion and subsequently failed to match the name 'Almaz-Antey Telecom' with the designated organisation 'Almaz-Antey'.[72] As a result, Cobham breached multiple provisions of the Ukraine-related sanctions regulations and received a $87,507 penalty.[73] Similarly, due to differences in punctuation and capitalisation, Apple Inc. used screening software that failed to match 'SIS DOO' in their internal data with the alleged narcotics trafficker 'SIS d.o.o', resulting in multiple unauthorised payments between 2014 and 2017.[74] Further, an online money transmitter, Payoneer Inc. ('Payoneer'), failed to detect 2,260 violations of multiple sanctions regulations, including in relation to weapons of mass destruction, as weak algorithms automatically discounted close name variations.[75]

Regulated entities can also fail to detect sanctioned parties where an automated system does not screen against the other relevant datapoints included in the regulation other than the name, such as the location, alias and additional identifying information provided by the regulator. Two recent enforcement actions exemplify this risk. In the Payoneer action discussed above, a RegTech tool failed to screen the business identifier codes and locations of their customers, despite the codes and locations appearing in the sanctions lists, which contributed to the 2,260 undetected sanctions violations.[76] In a second action, Amazon.com Inc failed to screen their location data accurately where a city within a sanctioned jurisdiction or a spelling variation of a sanctioned country was screened in their internal data.[77] For example, if an address contained 'Yalta, Krimea', the system did not recognise that 'Yalta' is a city in Crimea or that the alternate spelling of Crimea had been used in the address

[67] See, e.g., Parker, "Reinventing Regulation within the Corporation," 533; Parker, "Compliance Professionalism and Regulatory Community," 215–239; Braithwaite, "The New Regulatory State," 222–238.
[68] van Rooij, "Introduction," 1.
[69] Parker, "The Challenge of Empirical Research," 56–58.
[70] Parker, "The Challenge of Empirical Research," 57.
[71] van Rooij, "Introduction," 1. See also Parker, "The Challenge of Empirical Research," 45.
[72] United States Department of Treasury, "Cobham Holdings."
[73] United States Department of Treasury, "Cobham Holdings."
[74] United States Department of Treasury, "Apple, Inc. Settles."
[75] United States Department of Treasury, "OFAC Enters Into $1,385,901.40 Settlement."
[76] United States Department of Treasury, "OFAC Enters Into $1,385,901.40 Settlement."
[77] United States Department of Treasury, "OFAC Settles with Amazon.com."

field.[78] In these circumstances, the rules-based algorithms were unable to detect the sanctioned entities because of their system configuration and behaviour.

Regulated entities can also encounter issues where they do not upload all relevant data into a system, and thus fail to use the system in a way that correctly aligns with their legal obligations. For example, MoneyGram Payments Systems Inc (MoneyGram) failed to detect that the federal inmates processing payments through their transfer services were designated individuals, due to a mistaken belief that they were not required to screen the inmates under their agreement with the Federal Bureau of Prisons.[79] In this instance, MoneyGram relied on their sanctions screening software to detect sanctioned parties but decided not to upload the federal inmates for screening; consequently, there was no way to identify sanctions risk across these payments.[80] Where an organisation misunderstands its legal obligations and erroneously decides not to screen certain stakeholders or transactions, that organisation is at risk of repeatedly violating sanctions law, regardless of the level of sophistication of the screening tool.

An even deeper source of legal risk arises because some statutory norms may not be susceptible to codification and digitalisation. Progress has been made towards automating parts of the statutory interpretation process; however, despite decades of research, scholars of artificial intelligence and law have yet to devise computational models that comprehensively implement this process.[81] Disconnects between the code and algorithms used in automated systems and expectations of statutory interpretation cannot be entirely eliminated, particularly for statutory provisions that are discretionary, vague and syntactically and/or semantically ambiguous.[82] This is relevant to Australian sanctions compliance regulations, which, as is elaborated in Section 4.3, contain open-textured terms, such as 'reasonable precautions' and 'due diligence'. As exemplified by Services Australia's online compliance intervention, colloquially known as 'robodebt', the miscoding of statutory norms in ADM can generate significant legal risks, and in one instance, led to a class action settlement against the Australian Government worth more than AUD$1.8 billion.[83]

Additional legal risks can arise from biases in the code or data on which automated compliance decisions are based.[84] Like other forms of ADM, sanctions screening technologies are at risk of perpetuating race- and gender-based discrimination due to biased coding choices or historical human biases reflected in the data sets upon which machine-learning algorithms are trained.[85] Data from the consolidated sanctions lists contain information on names, addresses, race, gender and ethnicity.[86] In addition, digital profiles on designated individuals in research undertaken by RegTech providers may include other information that can form a basis for discrimination, such as family connections, work history and court appearances.[87] Moreover, in the sanctions context, biases may arise from the data generated from the Australian consolidated sanctions list, which reflects Australia's broad policy goals to align with westernised countries and designate individuals and entities from non-westernised countries, such as Iran and North Korea. Notably, automated systems have the potential to apply a biased decision-making logic to a very high volume of decisions.[88]

The potential bias risks associated with ADM are compounded by the opacity of 'black-box' automated systems.[89] The 'black-box' problem describes a situation in which the internal decision-making logic and mechanism of automated systems and the choices made in selecting the data and programming the system are unobservable or inherently opaque.[90] The rationale underpinning these decisions may be practically impossible to explain, meaning that regulated entities cannot analyse and critique the artificial reasoning processes used in their own compliance program.[91] As a result, machine-learning algorithms in

[78] United States Department of Treasury, "OFAC Settles with Amazon.com."
[79] United States Department of Treasury, "OFAC Enters Into $34,328.78 Settlement."
[80] United States Department of Treasury, "OFAC Enters Into $34,328.78 Settlement."
[81] Ashley, "Artificial Intelligence and Legal Analytics," 54.
[82] Ashley, "Artificial Intelligence and Legal Analytics," Chapter 2; Huggins, "Addressing Disconnection," 1055. Under the strict separation of judicial power in the *Australian Constitution*, only the judiciary is able to conclusively interpret the legal meaning of statutory terms: *Corporation of the City of Enfield v Development Assessment Commission* (2000) 199 CLR 135, 153 (Gleeson CJ, Gummow, Kirby and Hayne JJ); *Attorney-General (NSW) v Quin* (1990) 170 CLR 1, 36 (Brennan J).
[83] *Prygodicz v Commonwealth of Australia [No 2]* [2021] FCA 634.
[84] Huggins, "Addressing Disconnection," 1064.
[85] See, e.g., Barocas, "Big Data's Disparate Impact," 695; Chander, "The Racist Algorithm?," 1023.
[86] Wolfsberg Group, "Wolfsberg Guidance on Sanctions Screening," 7. See also Department of Foreign Affairs and Trade, "Australia and Sanctions."
[87] See Wolfsberg Group, "Wolfsberg Guidance on PEPs," 7.
[88] Huggins, "Addressing Disconnection."
[89] See, e.g., Barocas, "Big Data's Disparate Impact," 695; Chander, "The Racist Algorithm?," 1023; Pasquale, "The Black Box Society."
[90] See generally Pasquale, "The Black Box Society."
[91] Bathaee, "The Artificial Intelligence Black Box," 893.

the sanctions context can create decision-making rules and apply them to the users' data sets without a regulated entity understanding the parameters behind the decision, regardless of the organisation's technical expertise. This presents challenges for organisations to audit the rationale behind decisions and to detect errors within the reasoning, which in turn increases the risk of organisations unknowingly relying on system-generated decisions that incorporate erroneous or unethical considerations. As highlighted in the above analysis of the Payoneer action, this creates scope for a series of erroneous decisions produced by an undetected flawed logic, which exacerbates an organisation's exposure to regulatory compliance risks. As a result, organisations should exercise caution when relying on machine-learning outputs alone in the sanctions context.

4.3 Disconnects between RegTech and Regulatory Goals

In addition to its ability to promote rule compliance, RegTech can also be evaluated in terms of its alignment with the broader regulatory goals of the sanctions compliance framework.[92] Under s 16(7) of the *Autonomous Sanctions Act 2011* (Cth), a body corporate commits an offence if it cannot prove on the balance of probabilities that it took reasonable precautions and exercised due diligence to prevent the breach of a sanctions law.[93] 'Reasonable precautions' and 'due diligence' are undefined in the Act, giving these concepts the elasticity required to apply to a wide range of different circumstances.[94] The defence involves an objective test that requires the body corporate to demonstrate that it took precautionary steps that could reasonably be expected from a body corporate in the same position.[95] There has been limited judicial consideration of what 'reasonable precautions' and 'due diligence' require in this context, and there is no prescribed method to satisfy these tests.[96] This encourages organisations to adopt their own tailored, risk-based approach to sanctions compliance depending on their size, industry, geographical locations and their operations, and is ultimately intended to promote an overall 'culture of corporate compliance' with sanctions law.[97] This raises a critical question as to the relationship between RegTech tools and the promotion of a culture of corporate compliance as a key regulatory goal of the Australian sanctions regulatory framework.

There is no universally accepted definition of corporate culture. The concept carries different context-specific meanings across multiple academic disciplines.[98] As the optimum compliance culture will inevitably differ between organisations and regulatory environments, it is very difficult to land upon a clear, standardised definition of a 'culture of compliance' that applies in all circumstances. In contexts in which a failure to implement and uphold a 'culture of compliance' is enshrined in legislation, such as in the *Criminal Code Act 1995* (Cth),[99] cartel law[100] and ozone protection,[101] the term has been described in academic commentary as 'uncertain',[102] 'conceptually imprecise',[103] incapable of being measured objectively[104] and 'inherently slippery'.[105]

A valuable reference point for defining a culture of compliance in the Australian regulatory context is the definition of 'corporate culture' in the *Commonwealth Criminal Code Act 1995* (Cth). The term is defined as any 'attitude, policy, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities take place'.[106] This is a far-reaching, broad definition of corporate culture that classifies any policy, procedure or course of conduct as a component of organisational culture, including objective factors, such as written rules and documented procedures.[107] Similarly, within the Australian regulatory context, Greg Medcraft, a former ASIC chairman, described 'corporate culture' as encapsulating both the 'shared values and assumptions' that reflect the underlying 'mindset of an organisation', as well as the governance structures and internal controls, such as policies, procedures, courses of conduct and practices, which shape an organisation's mindset and behaviour.[108]

[92] See Section 4.1 above.
[93] *Autonomous Sanctions Act 2011* (Cth) s 16(7).
[94] For the range of contextual considerations relevant to building sanctions screening procedures, see Australian Banking Association, "ABA Sanctions Guidelines," 7.
[95] Australian Law Reform Commission, "Final Report," 260–261.
[96] Replacement Explanatory Memorandum, Autonomous Sanctions Bill 2010, 2.
[97] Autonomous Sanctions Bill 2010 Replacement Explanatory Memorandum, 2.
[98] Colvin, "Corporate and Personal Liability," 30.
[99] *Criminal Code Act 1995* (Cth) s 12.3(6).
[100] *Criminal Code Act 1995* (Cth) ss 12.3(2)(c)–(d).
[101] *Ozone Protection and Synthetic Greenhouse Gas Management Act 1989* (Cth) s 65.
[102] Colvin, "Corporate and Personal Liability," 40.
[103] O'Brien, "Regulating Culture," xv, xxvi–xxvii.
[104] Westbrook, "The Culture of Financial Institutions," 57.
[105] Awrey, "Between Law and Markets," 205.
[106] *Criminal Code Act 1995* (Cth) s 12.3(6).
[107] *R v Potter & Mures Fishing Pty Ltd* (Transcript, Supreme Court of Tasmania, Blow CJ, 14 September 2015) 464, 465.
[108] Medcraft, "The Importance of Corporate Culture in Improving Governance and Compliance," 1, 5.

For the purposes of this article, the preferred definition of a culture of compliance is a set of attitudes and behaviours that are predisposed towards compliance with applicable regulatory requirements and continually interact with the compliance rules, operations and procedures within an organisation.[109] This approach transcends a narrow emphasis on the existence or content of compliance policies and procedures, and includes how they are 'understood and applied' by individuals in the organisation.[110] Outside assessing written rules and procedures as indicators of compliance culture, organisations may also look to recordings of meetings,[111] reactions to past violations, incentives for lawful behaviour, the nature of offences committed,[112] the ongoing monitoring of digital technology performance and 'what people do when no one is watching'.[113] However, it is important to recognise that there is often a distinction between the 'façade of compliance' presented by corporate policy and the real corporate culture. The actual views, attitudes and habits within organisations often bear little resemblance to the version of corporate culture deducible from official corporate documents.[114] Parker and Gilad argue that the social reality of compliance is broader than system implementation or the content of policy documents and requires a more holistic consideration of compliance as a concept that encapsulates other social contextual factors in the organisation that are not codified or tangible.[115] Understanding these social contextual factors is ultimately an empirical question, which is a valuable avenue for future research, but is beyond the scope of the present legal analysis.

From the latter vantage point, a question arises as to the extent to which RegTech can contribute to fostering a culture of compliance. A culture of compliance includes continuously interacting with compliance operational guidelines and procedures,[116] which may incorporate RegTech components. In addition, a culture of compliance requires active organisational engagement with the network of written policies and procedures within an organisational compliance program, such as system maintenance procedures and processes, internal compliance manuals and legal risk assessments. These organisational compliance policies and procedures may reflect an interpretation of regulatory requirements that incorporate non-legal factors relevant to the broader context of the organisation.[117] The ongoing monitoring of digital technology performance can be automated, and the legal and regulatory instruments creating compliance requirements may be amenable to partial or full digitalisation.[118] This article suggests that where RegTech is included in a compliance program, a culture of compliance requires an organisational mindset towards compliance with regulatory requirements that is continually interacting with the use and maintenance of RegTech systems. However, other aspects of corporate culture, including values, attitudes and ethos, are human-centric and require the consideration of subjective, value-laden concepts, which are not decisions that are typically suited to automation.[119] In evaluating the potential role for RegTech in contributing to a culture of compliance, it is thus useful to distinguish between the objective, written elements of compliance programs, which may be amenable to digitalisation, and the subjective, cultural elements of compliance, which cannot be fully automated. As a result, RegTech can only ever provide a partial contribution to the broader regulatory goal of fostering a culture of corporate compliance.

5. Aligning Regulatory Technology, Rules and Goals

Where disconnects between RegTech and sanctions compliance expectations exist, options to facilitate alignment between the two ought to be explored. This section argues that ongoing human interaction with sanctions RegTech is needed to promote alignment between regulatory technology, rules and goals.

The analysis in Section 4 underscores that Australian organisations should not rely on automated systems alone to detect sanctioned parties in their internal data without human oversight and a holistic understanding of how the system algorithms operate and behave.[120] This relies on organisations creating a culture in which staff are analysing algorithmic outputs, including fuzzy-logic parameters, and ensuring that all the identifying information in a sanctions list is being accurately screened against their internal data.[121] The enforcement actions also demonstrate that technology cannot provide the entire solution for

[109] French, "The Culture of Compliance," 20.
[110] *Australian Securities and Investments Commission v Chemeq Ltd* (2006) 234 ALR 511, [85] (French J).
[111] Belcher, "Imagining How A Company Thinks," 21.
[112] Bucy, "Corporate Ethos," 91.
[113] Commonwealth of Australia, "Royal Commission," 334.
[114] Fisse, "Penal Designs and Corporate Conduct," 290; Hill, "Legal Personhood and Liability."
[115] Parker, "Internal Corporate Compliance Management Systems," 179.
[116] French, "The Culture of Compliance," 4.
[117] Edelman, "Working Law;" Edelman, "To Comply or not to Comply," 110.
[118] Huggins, "Addressing Disconnection," 1060.
[119] In relation to automating discretionary requirements requiring the weighing of different factors and values, see Perry, "iDecide."
[120] United States Department of Treasury, "OFAC Enters Into $1,385,901.40 Settlement;" United States Department of Treasury, "OFAC Settles with Amazon.com."
[121] United States Department of Treasury, "MID-SHIP Group LLC Settles."

demonstrating compliance in this area. Rather, any system must be supported by internal structures and a culture of compliance to identify system errors and mitigate the risk of unknowingly breaching sanctions laws due to such errors. This further highlights the need for humans and technology to work in tandem to accurately, efficiently and meaningfully drive compliance with legal requirements.

The expectation that regulated entities understand and monitor RegTech system behaviour can create significant issues. In particular, the 'black-box' problem prevents individuals from accurately unveiling the true reasons behind algorithmic outputs, particularly from machine learning, creating impediments for system monitoring and review. However, these challenges do not dilute the need to continually analyse system behaviour.[122] ADM tools ought to be deployed within a culture of compliance in which individuals are encouraged to question the accuracy of the automated outputs and to raise any concerns that are identified upon the review of those results. This culture combats the aura of mechanical infallibility that often emanates from system-generated outcomes, which causes individuals to perceive system-generated results to be correct and defer to them accordingly.[123] The critical evaluation of automated inputs and outputs can assist organisations to identify errors that may evidence automation bias or misguided decision making that emphasises irrelevant factors.

This article argues that to ensure its optimal performance, RegTech must be embedded within a culture of compliance with applicable regulations whereby humans continually interact with the software to ensure it consistently promotes legal compliance objectives. A key lesson learned from the use of RegTech in the sanctions context is that a compliance program must be regularly reviewed to ensure its alignment with the relevant legal requirements. If RegTech is not supplemented by an accurate understanding of the relevant law, as identified in the OFAC enforcement action against MoneyGram, multiple breaches of sanctions law may occur, exposing organisations to financial penalties and potential reputational damage.[124] The correct alignment depends on a sound understanding of regulatory requirements being embedded into official procedures and an organisation's culture in which system maintenance procedures are understood and applied by individuals in a way that aligns with the regulations. This also speaks to active organisational engagement with sanctions regulations across the organisation, from senior management to operational compliance professionals, whereby senior management set the tone and actively promote a culture of compliance with the law that permeates all levels of the organisation.[125]

Another lesson learned from the sanctions context is the need for a culture of compliance to underpin all human interactions with the system, including system monitoring, system audits and internal data preparation. A failure to configure a system in a way that accurately automates compliance decisions may result in continuous breaches of the relevant law, as seen in the OFAC enforcement action against Payoneer in which 2,276 breaches stemmed from configuration issues in their sanctions screening technology.[126] This reveals that the expectation of regulators goes beyond simply implementing a digital solution and extends to the continual monitoring of system behaviour. This lesson is transferable to other regulatory contexts, as it demonstrates the broader potential for multiple breaches of regulatory requirements if the calibration of the system contains undetected errors. Thus, RegTech solutions must sit within an organisational culture in which individuals in the organisation hold a shared set of attitudes, values and behaviours towards compliance that is manifested in the way in which automated systems are designed, used, monitored and reviewed.

6. Conclusion

Sanctions compliance requirements are complex and subject to rapid change. *Prima facie*, RegTech offers an attractive solution for enhancing the efficiency, consistency and cost effectiveness of the sanctions compliance processes of organisations. However, significant risks can arise from RegTech solutions that fall short of meeting regulatory expectations. Unsophisticated RegTech solutions can increase the legal and reputational risks of organisations and undermine broader compliance goals.

Differentiating between compliance with regulatory rules and broader regulatory goals highlights diverse technical and legal disconnects between RegTech and sanctions compliance requirements. As exemplified by a spate of recent sanctions enforcement actions in the US involving flawed RegTech systems, RegTech solutions can be misaligned with regulatory rules as a result of coding errors, incomplete data sets and the digital mistranslation of regulatory requirements. Moreover, RegTech will, at best, only ever provide a partial contribution to the broader regulatory goal of fostering a culture of corporate

[122] Bathaee, "The Artificial Intelligence Black Box," 901–905.
[123] Huggins, "Addressing Disconnection," 1067–1068.
[124] United States Department of Treasury, "OFAC Enters Into $34,328.78 Settlement."
[125] See Office of Foreign Assets Control, "A Framework," 3; French, "The Culture of Compliance," 4.
[126] United States Department of Treasury, "OFAC Enters Into $1,385,901.40 Settlement."

compliance. This article has argued that human interactions with and the oversight of well-calibrated RegTech tools are needed if such tools are to meaningfully enhance compliance with both regulatory rules and goals in the sanctions context.

For optimal outcomes, RegTech should be embedded within a broader culture of compliance in which individuals are committed to an ethical framework and engage in the ongoing assessment of the alignment of automated systems with the regulatory compliance objectives. Thus, automating elements of compliance processes should not be perceived as reducing the need for human analysis in compliance. Rather, there is an important complementary role for both automation and human analysis to best achieve compliance with applicable regulatory requirements. Future empirical research is needed regarding how key organisational actors interpret and implement automated compliance solutions in response to legal complexity and ambiguity.[127] Such analyses will further enrich understandings of how RegTech can enhance both rule compliance and substantive compliance in sanctions and other diverse regulatory contexts.

[127] See, e.g., Edelman, "Working Law;" Edelman, "To Comply or not to Comply," 103.

Bibliography

Secondary Sources

Anagnostopoulos, Ioannis. "FinTech and RegTech: Impact on Regulators and Banks." *Journal of Economics and Business* 100 (2018): 7–25. https://doi.org/10.1016/j.jeconbus.2018.07.003.

Arner, Douglas W., Jànos Barberis, and Ross P. Buckley. "FinTech, RegTech, and the Reconceptualization of Financial Regulation." *Northwestern Journal of International Law and Business* 37, no 3 (2017): 370–414.

Arner, Douglas W., Jànos Barberis, and Ross P. Buckley. "FinTech and RegTech in a Nutshell, and the Future in a Sandbox." *CFA Institution Research Foundation* 3, no 4 (2017): 1–20. http://dx.doi.org/10.2139/ssrn.3088303.

Ashley, Kevin. *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age.* Cambridge: Cambridge University Press, 2017.

Australian Banking Association. *ABA Sanctions Guidelines: A Guide to Industry Practice*. (Australian Banking Association, 2021).

Australian Law Reform Commission. *Corporate Criminal Responsibility: Final Report*. (Australian Law Reform Commission, 2020).

Australian Securities and Investment Commission (ASIC). *ASIC's Innovation Hub and Our Approach to Regulatory Technology* (ASIC, 2017).

Awrey, Dan, William Blair, and David Kershaw. "Between Law and Markets: Is There a Role for Culture and Ethics in Financial Regulation?" *Delaware Journal of Corporate Law* 38, no 1 (2013): 191–245.

Bamberger, Kenneth A. "Technologies of Compliance: Risk and Regulation in a Digital Age." *Texas Law Review* 88, no 4 (2010): 669–739.

Barocas, Solon and Andrew D. Selbst. "Big Data's Disparate Impact." *California Law Review* 104 (2016): 671–732.

Bathaee, Yavar. "The Artificial Intelligence Black Box and the Failure of Intent and Causation." *Harvard Journal of Law and Technology* 31, no 2 (2018): 879–938.

Belcher, Amy. "Imagining How a Company Thinks: What is Corporate Culture?" *Deakin Law Review* 11, no 2 (2006): 1–21.

Bennett Moses, Lyria. "How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target." *Law, Innovation and Technology* 5, no 1 (2013): 1–20. https://doi.org/10.5235/17579961.5.1.1.

Boston Consulting Group and RegTech Association, "Australia's Global RegTech Hub Poised for Growth: A Perspective on Supporting the Local RegTech Sector to Scale." October 27, 2020. https://www.bcg.com/publications/2020/australia-global-regtech-hub-poised-for-growth.

Braithwaite, John. "The New Regulatory State and the Transformation of Criminology." *British Journal of Criminology* 40, no 2 (2000): 222–238. https://doi.org/10.1093/bjc/40.2.222

Brownsword, Roger. "The Challenge of Regulatory Connection." In *Rights, Regulation, and the Technological Revolution*, 160–184. Oxford: Oxford University Press, 2008.

Bucy, Pamela H. "Corporate Ethos: A Standard for Imposing Corporate Criminal Liability." *Minnesota Law Review* 75 (1991): 1095-1184.

Chander, Anupam. "The Racist Algorithm?" *Michigan Law Review* 115, no 6 (2017): 1023-1045.

Clark, Roger. "The Opportunities Afforded by RegTech: A Framework for Regulatory Information Systems." November 14, 2018. http://www.rogerclarke.com/EC/RTF.html.

Colvin, John H.C. and James Argent. "Corporate and Personal Liability for 'Culture' in Corporations?" *Companies and Securities Law Journal* 34, no 1 (2016): 30-47.

Commonwealth of Australia. *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry: Final Report*. (Commonwealth of Australia, 2019).

C6 Intelligence. "Technology and Data Analysis for Global Sanctions Compliance." *Risk and Compliance Magazine*, July–September Issue, 2018. https://www.acurisriskintelligence.com/assets/RC_MiniRT%20Jul18_C6_Reprint.pdf.

Department of Foreign Affairs and Trade. "Australia and Sanctions: Consolidated List." https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list.

Dow Jones Risk and Compliance. *Leveraging Data and Technology for Sanctions Compliance: OFAC's 50% Rule*. (Dow Jones Risk and Compliance, 2018).

Drezner, Daniel W. "How Smart are Smart Sanctions?" *International Studies Review* 5, no 1 (2003): 107–110. https://doi.org/10.1111/1521-9488.501014

Edelman, Lauren B. *Working Law: Courts, Corporations, and Symbolic Civil Rights*. Chicago: University of Chicago Press, 2016.

Edelman, Lauren B. and Shauhin A. Talesh. "To Comply or Not to Comply—That Isn't the Question: How Organizations Construct the Meaning of Compliance." In *Explaining Compliance: Business Responses to Regulation*, edited by C. Parker and V. Lehmann Nielsen, 103-122. Cheltenham: Edward Elgar, 2011.

Fisse, Brent. "Penal Designs and Corporate Conduct: Test Results from Fault and Sanctions in Australian Cartel Law." *Adelaide Law Review* 40, no 1 (2019): 285–300.
French, Justice Robert. "The Culture of Compliance—A Judicial Perspective." *Federal Judicial Scholarship* 16 (2003). http://classic.austlii.edu.au/au/journals/FedJSchol/2003/16.html.
Grand View Research. *RegTech Market Size, Share and Trends Analysis Report by Organisation Size, By Application (Risk and Compliance Management, Identity Management), By Region, and Segment Forecasts, 2019–2025* (Grand View Research, 2019).
Hildebrandt, Mireille. "Algorithmic Regulation and the Rule of Law." *Philosophical Transactions of the Royal Society* 376, no 2128 (2018): 1-11. https://doi.org/10.1098/rsta.2017.0355.
Hill, Jennifer. "Legal Personhood and Liability for Flawed Corporate Cultures." (Research Paper No 19/03, Faculty of Law, The University of Sydney, February 2019).
HM Treasury and Office of Financial Sanctions. "Enforcement of Financial Sanctions." https://www.gov.uk/government/collections/enforcement-of-financial-sanctions.
Huggins, Anna. "Addressing Disconnection: Automated Decision-Making, Administrative Law and Regulatory Reform." *UNSW Law Journal* 44, no 3 (2021): 1048–1077.
Illieva, Jana, Aleksandar Dashtevski and Filip Kokotovic. "Economic Sanctions in International Law." *UTMS Journal of Economics* 9, no 2 (2018): 201–2011.
Johansson, Ellinor, Konsta Sutinen, Julius Lassila, Valter Land, Minna Martikainen, and Othmar M. Lehner. "RegTech—A Necessary Tool to Keep Up with Compliance and Regulatory Changes?" *ACRN Journal of Finance and Risk Perspectives* 8 (2019): 71–85.
Johnson, Wayne. "The Evolution of Sanctions and the Role of Technology." September 16, 2019. https://internationalbanker.com/technology/the-evolvement-of-sanctions-and-the-role-of-technology/.
Kerrigan, Christopher, James Campbell, Cindy McNair, and Andrew Wilcock. "Sanctions Regime, Practical Issues and Steps You Should Take." February 23, 2022. https://www.allens.com.au/insights-news/insights/2020/09/sanctions-regime-in-australia/.
Market Research Store. *Sanctions Screening Software Market Research Report 2021–2028*. (Market Research Store, 2021).
Medcraft, Greg. "The Importance of Corporate Culture in Improving Governance and Compliance." Challenger Legal and Corporate Affairs team offsite, Sydney, July 28, 2016. https://download.asic.gov.au/media/3964314/greg-medcraft-speech-challenger-offsite-28-july-2016.pdf.
Ministry of Foreign Affairs of the Russian Federation. "Foreign Ministry Statement on Personal Sanctions Against Representatives of Australian Military Command, Business Leaders and Journalists." *The Ministry of Foreign Affairs of the Russian Federation*, June 16, 2022. https://www.mid.ru/en/foreign_policy/news/1818118/.
O'Brien, Justin and George P. Gilligan. "Regulating Culture: Problems and Perspectives." In *Integrity, Risk and Accountability in Capital Markets*, edited by Justin O'Brien and George P. Gilligan, xv-xxx. Oxford: Hart, 2013.
Office of Foreign Assets Control. "A Framework for OFAC Compliance Commitments." *Department of the Treasury*, 2 May 2019. https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.
Packin, Nizan Geslevich. "RegTech, Compliance and Technology Judgment Rule." *Chicago-Kent Law Review* 93, no 1 (2018): 207–208.
Parker, Christine. "Compliance Professionalism and Regulatory Community: The Australian Trade Practices Regime." *Journal of Law and Society* 26, no 2 (1999): 215–239. https://doi.org/10.1111/1467-6478.00123.
Parker, Christine. "Reinventing Regulation within the Corporation: Compliance-Orientated Regulatory Innovation." *Administration and Society* 32, no 5 (2000): 529–565. https://doi.org/10.1177/00953990022019579.
Parker, Christine and Sharon Gilad. "Internal Corporate Compliance Management Systems: Structure, Culture and Agency." In *Explaining Compliance: Business Responses to Regulation*, edited by Christine Parker and Vibeke Lehmann Nielson, 170-195. Cheltenham: Edward Elgar, 2011.
Parker, Christine and Vibeke Nielsen. "The Challenge of Empirical Research on Business Compliance in Regulatory Capitalism." *Annual Review of Law and Social Science* 5, no 1 (2009): 45–70. https://doi.org/10.1146/annurev.lawsocsci.093008.131555.
Pasquale, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard: Harvard University Press, 2015.
Perry, Justice Melissa. "iDecide: Administrative Decision-Making in the Digital World." *Australian Law Journal* 91 (2017): 29–30.
Portela, Clara. "National Implementation of United Nations Sanctions." *International Journal* 65, no 1 (2009): 13–30.
Ruys, Tom. "Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework." In *Research Handbook on UN Sanctions and International Law*, edited by Larissa van den Herik, 19-51. Cheltenham: Edward Elgar, 2016.
Silverberg, Kristen, Andrés Portilla, Conan French, Bart van Liebergen, and Stephanie Van Den Berg. "RegTech in Financial Services: Technology Solutions for Compliance and Reporting." (Institute of International Finance, 2016).

Singh, Charanjit, Wangwei Lin and Zhen Ye. "Can Artificial Intelligence, RegTech and CharityTech Provide Effective Solutions for Anti-Money Laundering and Counter-terror Financing Initiatives in Charitable Fundraising." *Journal of Money Laundering Control* 24, no 3 (2020): 464-482. https://doi.org/10.1108/JMLC-09-2020-0100.

Surden, Harry. "Artificial Intelligence and Law: An Overview." *Georgia State University Law Review* 35, no 4 (2019): 1305–1337.

Tully, Stephen. "Australia's Autonomous Sanctions Regime: Problems and Prospects." *Australian Journal of Administrative Law* 20, no 3 (2013): 149-167.

Tully, Stephen. "Implementing Targeted Sanctions in Australia: A Role for Procedural Fairness." *Murdoch University Electronic Journal of Law* 16, no 1 (2009): 115–133.

United States Department of Treasury. "Apple, Inc. Settles Potential Civil Liability for Apparent Violations of the Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R. part 598." *United States Department of Treasury*, November 25, 2019. https://home.treasury.gov/system/files/126/20191125_apple.pdf.

United States Department of Treasury. "MID-SHIP Group LLC Settles Potential Civil Liability for Apparent Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations." *United States Department of Treasury*, May 2, 2020. https://home.treasury.gov/system/files/126/20190502_midship.pdf.

United States Department of Treasury. "OFAC Enters Into $1,385,901.40 Settlement with Payoneer Inc." *United States Department of Treasury*, July 23, 2021. https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf.

United States Department of Treasury. "OFAC Enters Into $34,328.78 Settlement with MoneyGram Payment Systems, Inc. for Apparent Violations of Multiple Sanctions Programs." *United States Department of Treasury*, April 29, 2021. https://home.treasury.gov/system/files/126/20210429_moneygram.pdf

United States Department of Treasury. "OFAC Settles with Amazon.com, Inc. with Respect to Potential Civil Liability for Apparent Violations of Multiple Sanctions Programs." *United States Department of Treasury*, July 8, 2020. https://home.treasury.gov/system/files/126/20200708_amazon.pdf.

United States Department of the Treasury. "2019 Enforcement Information." https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2019-enforcement-information.

United States Department of Treasury, Office of Foreign Asset Control. "Enforcement Information for November 27, 2018." https://ofac.treasury.gov/media/13401/download?inline.

van Rooij, Benjamin and D. Daniel Sokol. "Introduction: Compliance as the Interaction between Rules and Behaviour." In *The Cambridge Handbook of Compliance*, edited by Benjamin van Rooij and D. Daniel Sokol, 1-12. Cambridge: Cambridge University Press, 2021.

Wang, Amy. "The Role of Regtech in Augmenting Regulatory Compliance: Regulating Technology, Accountability and Liability." *University of New South Wales Law Journal Student Series* 10 (2019). http://classic.austlii.edu.au/au/journals/UNSWLawJlStuS/2019/10.html.

Waye, Vicky. "RegTech: A New Frontier in Legal Scholarship." *Adelaide Law Review* 40, no 1 (2019): 363–386.

Weber, Rolf H., "RegTech as a New Legal Challenge." *The Capco Institute Journal of Financial Transformation* 46 (2017): 11.

Westbrook, David A. "The Culture of Financial Institutions: The Institution of Political Economy." In *Integrity, Risk and Accountability in Capital Markets: Regulating Culture*, edited by Justin O'Brien and George Gilligan, 3-20. Cheltenham: Hart, 2013.

White & Case, "The Emergence of AI RegTech Solutions for AML and Sanctions Compliance." *Risk and Compliance Magazine*, April–June Issue, 2017. https://www.whitecase.com/publications/article/emergence-ai-regtech-solutions-aml-and-sanctions-compliance.

Wolfsberg Group. *Wolfsberg Guidance on Politically Exposed Persons (PEPs).* (Wolfsberg Group, 2017).

Wolfsberg Group. *Wolfsberg Guidance on Sanctions Screening*. (Wolfsberg Group, 2019).

Wyld, Robert and Lara Douvartzidis. *Sanctions 2021: International Comparative Legal Guides* (Johnson Winter Slattery, 2021).

Yeung, Karen. *Securing Compliance: A Principled Approach*. Oxford: Hart, 2004.

Zeranki, Stefan and Ibrahim E Sancak. "Digitalisation of Financial Supervision with Supervisory Technology (SupTech)." *Journal of International Banking Law and Regulation* 8 (2020): 309-329.

Primary Legal Material

ASIC v Flugge & Geary [2016] VSC 779

Attorney-General (NSW) v Quin (1990) 170 CLR 1

Australian Securities and Investments Commission v Chemeq Ltd (2006) 234 ALR 511

Autonomous Sanctions Act 2011 (Cth)

Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 (Cth)

Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Regulations 2021 (Cth)
Autonomous Sanctions Amendment (Russia) Regulations 2022 (Cth)
Autonomous Sanctions Amendment (Ukraine Regions) Regulations 2022 (Cth).
Autonomous Sanctions (Designated Persons and Entities and Declared Persons—Russia and Ukraine) List 2014 (Cth)
Autonomous Sanctions (Export Sanctioned Goods—Russia) Designation 2022 (Cth)
Autonomous Sanctions (Import Sanctioned Goods—Russia) Designation 2022 (Cth)
Autonomous Sanctions Regulations 2011 (Cth)
Charter of the United Nations Act 1945 (Cth)
Corporation of the City of Enfield v Development Assessment Commission (2000) 199 CLR 135
Criminal Code Act 1995 (Cth)
Ozone Protection and Synthetic Greenhouse Gas Management Act 1989 (Cth)
R v AA (No 3) [2019] NSWSC 1982
R v Choi (No 10) [2021] NSWSC 891
R v Potter & Mures Fishing Pty Ltd (Transcript, Supreme Court of Tasmania, Blow CJ, 14 September 2015) 464
Replacement Explanatory Memorandum, Autonomous Sanctions Bill 2010
Prygodicz v Commonwealth of Australia [No 2] [2021] FCA 634