Between privacy and protection

A proportionality based privacy framework for AML/CFT in Dutch Banking

Master Thesis
Engineering and Policy Analysis

S. Uffing

TU Delft

Between privacy and protection

A proportionality based privacy framework for AML/CFT in Dutch Banking

by

S. Uffing

Student number:	4933192	
Project duration:	February 10, 2025 – July 14, 2025	
Thesis committee:	Dr. U. Pesch,	TU Delft, Chair
	Dr. J.M. Duran	TU Delft, Supervisor
	Dr. M. Tuler de Oliveira	TU Delft, Supervisor
	C. Tabaouni MSc	KPMG the Netherlands

Cover: Adobe Stockfoto, Money laundering

Preface

When I began the process of writing this thesis, I could never have imagined that it would take the form it has now. During my studies, I was most drawn to the technical courses, and I expected my final thesis to reflect that interest. My ambition was to develop a complex model that would showcase the sophisticated analytical techniques I have acquired over the past five years. The AML/CFT domain seemed like the perfect environment to do so, as it was rich in data and filled with opportunities for advanced analytical techniques.

My initial plan was straightforward: select a modelling approach, zoom in on a specific parameter, and optimize it to improve model accuracy. However, as I delved deeper into the literature, I repeatedly encountered the same pattern: each paper presented a promising modelling technique, reported improvements in parameters X, Y, and Z, and then concluded that the approach could not be implemented due to privacy concerns.

In retrospect, this realization marked the most important decision point of this research: Ignore the problem and proceed with the original plan, or embrace the issue and focus on solving a real policy obstacle instead. If privacy is the main barrier to innovation in the AML/CFT field, then shouldn't we address that barrier before fine-tuning the models?

While 'overcoming' the privacy barrier is what initially motivated this research, I have come to realize over the past months that viewing privacy solely as an obstacle to be overcome is about as unproductive as ignoring it entirely. Privacy is a complex and evolving concept that can have a tremendous impact on our society. Attempting to bypass it without careful reflection does not lead to meaningful or sustainable innovation.

This continuous reflection led to the fact that this thesis is not a typical EPA thesis product. It draws on legal analysis, philosophical theory, and institutional design rather than quantitative analysis. While the absence of numerical results and a closed research cycle leaves me somewhat dissatisfied, I ultimately feel content with my choice to engage seriously with the complexity of this concept, instead of simplifying it to produce another coherent, yet incomplete story. This led to the insight that maybe the most sophisticated modelling skill I have learned through the last years, is knowing when, and when not to build a model.

During the process of writing this thesis I have received amazing guidance in which there was room for my own ideas and the expertise to steer the product to a scientifically finished research. The ability of my counsellors to guide and inspire, while keeping a spark of creativity alive created a pleasant and inspiring work environment. For this, I want to express my gratitude to the TU Delft supervisory board: Juan Manuel Duran, Marcella Tuler de Oliveira and Udo Pesch, and my KPMG thesis counsellor: Chaymae Tabaouini.

S. Uffing
Rotterdam, June 2025

Abstract

This thesis investigates the interplay between privacy and safety within the context of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) practices in the Dutch banking sector. As financial institutions face increasing pressure to detect and report Financial Economic Crime (FEC), the demand for advanced surveillance techniques such as: Artificial Intelligence (AI)-driven monitoring, Public Private Partnerships (PPPs) and cross-bank data sharing, has grown. However, these innovations face barriers in their implementation due to concerns regarding financial privacy and data protection.

By conducting a structural privacy assessment, this research identifies and categorizes the specific privacy harms that emerge from transaction monitoring. It analyses the tensions between key legal frameworks, including the General Data Protection Regulation (GDPR), the Dutch AML/CFT law (Wwft) and the recently introduced EU Anti Money Laundering Regulation (AMLR), highlighting the regulatory ambiguities and ethical dilemmas they present. Using expert interviews and a conceptual privacy framework grounded in academic theory, the study evaluates the proportionality of privacy and safety trade-offs.

The key message of this thesis is that successful AML/CFT will remain politically and technically fragile until banks, regulators and developers adopt a structured, continuously-revised understanding of privacy harms and use that lens to decide which monitoring practices, data-sharing schemes and analytic tools are ethically and legally proportionate. The thesis therefore supplies both an analytic privacy framework tailored to transaction monitoring and a map of the legal, technical and governance tensions that must be resolved before developments such as AI, data-sharing and PPPs can be deployed responsibly.

Keywords: *Privacy, Anti-Money Laundering, Counter Terrorism Financing, GDPR, Data-sharing, Public-Private Partnership, Artificial Intelligence*

Contents

List of Figures

List of Tables

Glossary

This report uses several abbreviations. Each term is written out in full when first introduced in a chapter; for convenience, all abbreviations are listed in the table below.

Abbreviations

AI	Artificial Intelligence
AI Act	Artificial Intelligence Act (EU)
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Authority (EU)
AMLR	Anti-Money Laundering Regulation
AP	Autoriteit Persoonsgegevens (Dutch Data Protection Authority)
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
DNB	De Nederlandsche Bank (Dutch Central Bank)
DPIA	Data Protection Impact Assessment
EPA	Engineering and Policy Analysis (TU Delft MSc programme)
ESG	Environmental, Social and Governance
EU	European Union
FATF	Financial Action Task Force
FEC	Financial Economic Crime
FIU	Financial Intelligence Unit
FIU-NL	Financial Intelligence Unit Netherlands
FIOD	Fiscale Inlichtingen- en Opsporingsdienst (Fiscal Intelligence and Investigation Service)
GDPR	General Data Protection Regulation
IMF	International Monetary Fund
KYC	Know Your Customer
MPC	Multi-Party Computation
OFAC	Office of Foreign Assets Control (United States)
OM	Openbaar Ministerie (Public Prosecution Service)
PPP	Public–Private Partnership
SDG	Sustainable Development Goals
TF	Transaction Filtering
TM	Transaction Monitoring
TMNL	Transactie Monitoring Nederland
UN	United Nations
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum (Research and Documentation Centre)
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme (Dutch AML/CFT Act)

1 Introduction

1.1. Social Relevance

Each year, an estimated 2-5 % of the world's GDP or roughly $800 billion to $2 trillion is funnelled through money-laundering schemes (United Nations Office on Drugs and Crime, 2023). By cycling illicit proceeds through seemingly legitimate transactions, criminals convert illegally acquired cash into seemingly legal spending power. In other words: money laundering is what makes crime pay. Terrorism financing abuses the financial system by using it to finance terroristic organizations. While the cash flows are estimated around $6.6 Billion, which is far lower than money laundering cash flows (Fitzpatrick and Lynch, 2016), financing of terrorism directly contributes to activities that disrupt society and therefore poses a major societal threat. Money laundering and terrorism financing both involve the abuse of the financial system and are therefore classified as forms of Financial Economic Crime (FEC). Due to the societal damage of FEC, for the last 50 years, international efforts have been made to detect and prevent FEC.

Financial institutions (FIs) such as: banks, insurance companies and payment services are given a key responsibility in Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT). FIs have a legal obligation to analyse transactions made through their services and report suspicious transactions to the Financial Intelligence Units (FIU). The FIU will then research the transactions and take forensic actions. When FIs fail to detect and prevent illicit transactions appropriately, they risk severe penalties and reputational harm. An example of this is the €775 million fine the Dutch bank ING received in 2018 (FIOD, 2018). On top of the high fines, maintaining effective AML/CFT frameworks is costly. Dutch banks alone reportedly spend around 1.4 billion euro per year on AML/CFT operations, a part of the costs are in the over 13 thousand analysts that are checking transactions for suspicious activity (Nederlandse Vereniging van Banken, 2024). The disproportion of these numbers is shown when they are compared with the numbers of the police force as displayed in figure 1.1. High costs and inefficient, manual checks create an incentive for banks to look for a more efficient way to comply with their reporting obligations.

The road to more efficient transaction monitoring is far from smooth. In July 2024, the data sharing initiative Transaction Monitoring the Netherlands (TMNL) got scaled down due to violations of upcoming EU Laws regarding privacy (NOS, 2024). TMNL used pseudonymized data sharing to potentially expose more sophisticated money laundering techniques. The upcoming European Anti-Money Laundering Regulation (AMLR) considers these type of data sharing too big of a privacy violation which caused the initiative to be scaled down. Another example of innovation that stagnated in the AML/CFT sector is the Bunq Artificial Intelligence(AI) case: The Dutch bank Bunq had a major disagreement with the Dutch AML enforcer De Nederlandsche Bank (DNB). Bunq was developing advanced AML/CFT models that made use of AI. DNB did not allow for the use of these types of models due to regulatory and privacy reasons. In response to this Bunq sued DNB. This whole process lasted over 4 years but eventually Bunq won the lawsuit and is now actively using AI in their AML systems (Bunq, 2022).

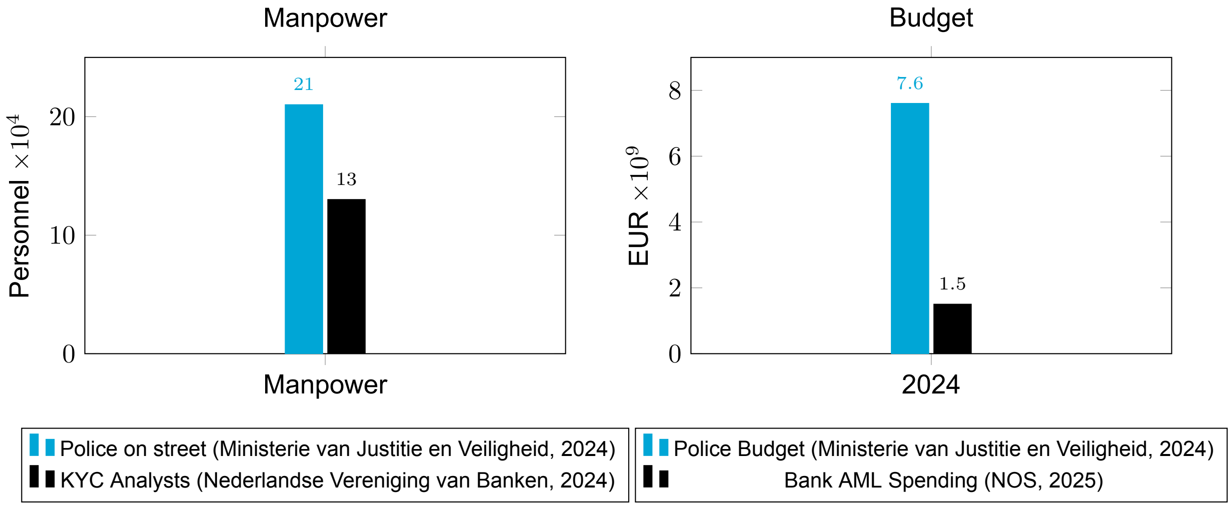

Figure 1.1: Comparison of manpower and budgets between police and AML operations

1.1.1. The dilemma

What the TMNL and the Bunq examples have in common is that development towards more effective transaction monitoring is facing privacy obstacles. FEC misuses the financial system to fund disruptors of society. Regulators want to prevent this, while leaving the financial system intact for legitimate purposes. At the same time, transaction data is sensitive and people treat it with great caution (Brits and Jonker, 2023). This presents a difficult choice for policymakers between privacy, growth and safety:

- **Privacy**
  Privacy is highly valued in society and even considered a human right (United Nations Office on Drugs and Crime, 2019), this also applies for financial data. First of all, data related to a bank account such as account number or the name and social security number can be linked directly to an individual and can therefore be considered as sensitive. On top of that, transactional data portrays a detailed image of an individuals behaviour. This means that violations of financial privacy can be harmful to both individuals and society
- **Growth**
  Part of the banks role in AML/CFT is freezing accounts or blocking transactions that carry a high risk of FEC. While this is necessary for blocking illicit cash flows, it can be a big inconvenience if legitimate transactions or accounts are blocked. The number of unrightfully frozen accounts is relatively low but due to the high impact of this action it is still relevant.
- **Safety**
  Is about preventing and detecting FEC. The thought behind this is that taking away funding and financial incentives of illegal activities would lead to a big discouragement of these activities or even make it impossible. The societal damage of criminality goes further than just the criminal actions. When organized crime reaches a certain scale it can undermine existing authorities. While this might seem far away, there is already literature that declares the Netherlands as a ’functioning narco state’ due to its high drug production and increasing corruption (Voeten, 2025). AML/CFT policy has the ultimate goal of increasing societal safety by reducing criminal resources. This goal is well represented in one of the first the anti-money laundering initiative that was taken in the United States. This operation got the code-name ’operation choke point’ because it had the purpose of squeezing the veins of criminal- or terrorist organizations.(Anthony, 2024)

All three of these factors are important, however an increase in one factor will likely lead to a decrease of at least one other factor. This is displayed when scenarios are drafted in which only two factors are considered:

1. It is completely possible to focus on only *growth* and collective *safety* without considering *privacy*. Mass surveillance of all transactions and big data analysis would lead to more available data and therefore more accurate models (safety), with a lower chance of unrightfully freezing accounts or

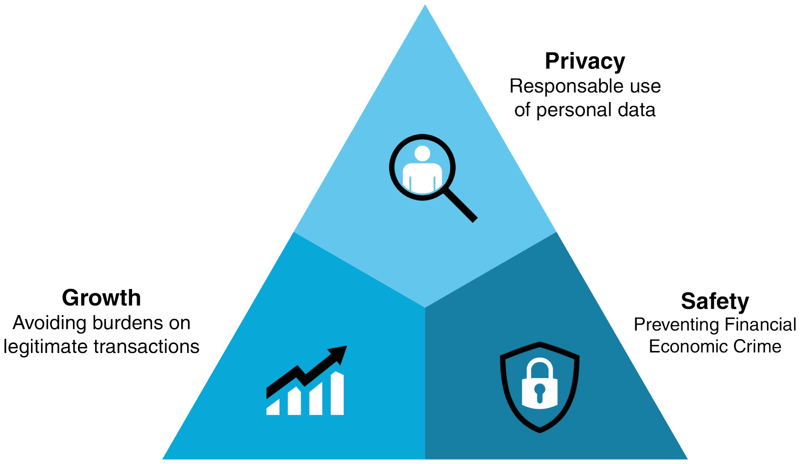
Privacy
Responsable use of personal data
Growth
Avoiding burdens on legitimate transactions
Safety
Preventing Financial Economic Crime

Figure 1.2: The AML/CFT trilemma between growth, privacy and safety

blocking transactions (growth). While it is no guarantee that full data availability would mean that the AML/CFT is flawless, it will still lead to an increase on both *growth* and *security*. However, this solution would imply mass surveillance which is a major privacy issue.

2. When a policy aims to respect *privacy* and *safety* system and is in disregard of *growth*, the solution is easy as well: Freezing all accounts would make money laundering impossible (safety) and requires no transaction monitoring (privacy). The downside here is that it is impossible for citizens to use the financial system, which would lead to a non-functional economy.
3. When leaving *safety* out of the picture the equation is also easily solved: Lay down all monitoring processes. This would mean that there is no surveillance (privacy) and that citizens can execute their business without being bothered (growth). This would also mean that transactions are not checked, which gives a free pass to the financing of criminality and terrorism (security).

These three extreme scenarios sketch the outlines of the presented 'trilemma'. The scenario without *growth* is a result of too much transaction filtering and the scenario without *safety* is a result of too little monitoring. More analysis of financial data could lead to more accurate models but this would be harmful to *privacy*. While neither of the three scenarios are desirable, there is a difference in how the scenario's are perceived. The ideas of a non-functional economy or a free playing field for terrorists and criminals have direct and concrete implications. The exact implications of mass surveillance on the other hand are still a bit abstract, some people might even be completely fine with mass surveillance for the sake of a safer world. This raises the question if sacrificing privacy is not just a necessary evil that has to occur for the sake of the other two societal benefits. This is typical for privacy; while it is seen as a fundamental right, defining it has proven very challenging (D. Solove, 2009).

On top of the lack of a clear definition, privacy is also something that is valued differently for every individual. One person might trade his privacy for a safer society without any doubt, while another takes great effort in preserving privacy and puts this above safety and financial growth. The definition and importance of privacy in an AML/CFT context are unclear. Nevertheless privacy is a main obstacle in developments towards a safer society. This incentivises further research about the relation between privacy and safety.

This research will define the role of privacy in an AML context and look into how it should weigh up against security and market functionality. The ultimate goal is to define guidelines for policy makers and banks to apply directly to emerging trends and asses whether the benefits of this trend weigh up against the harms.

1.1.2. Why the connection between ethics and technology is important

Modern technology has developed to the level where it can bridge dilemma's. Solar panels and windmills allow for energy production with decrease environmental impact, vaccines combat viruses that would otherwise have eradicated mankind and phones allow us to move far away from loved ones while still being able to talk to them whenever we want. Technology continues to amaze society everyday and it can sometimes seem like there is no limit to what can be achieved through innovation.

While technology is extremely powerful, there are things that cannot be solved through technology alone and face constraints in a different parts of society. These problems are bigger than equations and are inherently to optimize. In fact, properly defining these problems can sometimes even be impossible. These problems are also known as 'Wicked problems'. A wicked problem is a problem that is difficult to solve because of incomplete, contradictory and changing requirements that are often difficult to recognize (Johnston and Gulliver, 2022).

The privacy discussion in AML/CFT exemplifies a wicked problem. First of all, the solution direction is unclear. Maximizing privacy means minimizing money laundering effectiveness and vice versa. The balance has to be found between these two concepts but where this balance should be is dependent on individual values. Some stakeholders prioritize privacy, insisting that financial data remain as confidential as possible, while others argue that making sure that crime does not pay and terrorist attacks cannot be financed is far more important. The result is a dilemma requiring careful policy design that balances competing societal values.

Technology can be of great contribution in this. Privacy preserving techniques such as federated learning (Suzumura et al., 2022) and differential privacy (C. Xu et al., 2023) show great technological potential for privacy friendly AML/CFT solutions. However, without understanding of what it is that these technologies should preserve and to which extend, implementing this will never lead to the desired results. This means that while technology can eventually contribute to a more privacy friendly world, a understanding of the societal implication of privacy should be the starting point.

A clearer definition of privacy is also relevant for regulatory developments such as datasharing between banks or public-private partnerships (Hardouin, 2009). Recent regulatory developments, such as the EU's Anti-Money Laundering Regulation (AMLR), aim to strengthen cross-border collaboration but have also resulted in the scaling back of certain initiatives, including Transactie Monitoring Nederland (TMNL), due to compliance complexities (NOS, 2024).

On February 10th, 2025, the Dutch banking association submitted a proposal for the legalization of the exchange of information between obliged entities, competent authorities and law enforcement for public-private partnerships. The Dutch banking association emphasizes that information sharing is critical in ensuring effectiveness. Taking this to an international context, the European Banking Foundation has even stated:

> ”Weaknesses in information sharing between obliged entities, financial intelligence units and law enforcement authorities may inadvertently facilitate the activities of criminals who operate nationally or across borders.”

However, sharing financial data among multiple banks presents significant obstacles relating to confidentiality and legal constraints. High-profile efforts to consolidate transaction data have often stalled due to privacy concerns and regulatory uncertainties. Such barriers limit the effectiveness of AML efforts that could benefit from combined insights across various financial institutions.

These examples show that both technological and organizational developments do not lead to a solution in isolation. The societal aspect of AML/CFT and privacy needs to be perceived from a system perspective that combines a philosophical understanding of Privacy, a legal understanding of AML/CFT and data-protection laws and a technical understanding of AML/CFT models.

1.1.3. Sustainable development Goals(SDGs)

The SDGs represent the United Nations' blueprint for achieving a better and more sustainable future for all. In 2015 these 17 goals where adopted by all UN member states. The SDGs are designed to be achieved by 2030, providing a shared vision for countries. This research takes into account several of the SDGs which testifies to its social relevance.

SDG 16: Peace, Justice and Strong Institutions

The most direct alignment between AML research and the SDGs is with goal 16: Peace, Justice and Strong institutions. This goal is about promoting peaceful and inclusive societies for sustainable development, providing access to justice for all and build effective, accountable and inclusive institutions at all levels (United Nations, 2015). The sustainable development goals have indicators which break down the goal into more measurable targets.

Target 16.4: Combat organized crime and illicit financial flows The most direct link is with target 16.4. The target states that by 2030 the illicit financial and arms flows should be significantly reduced and that the recovery and return of stolen assets should be strengthened. This has the main purpose of combatting all forms of organized crime. The target directly backs up the urge to increase AML efficiency which shapes the dilemma between privacy and effectiveness. Privacy-preserving AML approaches contribute to this by:

- Enabling effective detection of suspicious transactions while respecting data protection principles
- Reducing the risk of financial surveillance overreach
- Building public trust in financial monitoring systems, increasing compliance
- Balancing security needs with fundamental rights

1.2. Scope

While every FI serves as a gatekeeper and is therefore responsible for the implementation of AML/CFT policy, this thesis focuses on AML/CFT in the banking system. This is due to the large amount of data that banks have available, the dependency users have on their banks and the means that banks have to directly apply innovation. As a location the Netherlands is chosen which also makes it relevant to the EU more broadly (given GDPR's European reach). As explained in Bakare et al. (2024), there are major differences in privacy regulations between the EU and the US. This should be taken into account when applying the findings from this research to a context outside of the EU. The intent is to compose privacy requirements specific to AML in a setting where most transactions are digitized and where strict data protection rules apply. While the results may serve as a reference point for non-EU contexts, cultural and legal differences mean that adaptations will likely be necessary.

Money laundering and the financing of terrorism are connected terms. Where money laundering has the purpose of making illegal acquired funds appear legal. Terrorism financing aims to use the banking system to support terroristic purposes. Both can be detected in similar ways and fall under the regulatory umbrella term of Financial Economic Crime (FEC). Since this thesis is about the balance between privacy and safety, it is applicable for both AML and CFT but it can zoom in on one of the two terms when practical examples are made.

1.3. Methodology

This thesis combines philosophical reflection with empirical insight to show how Anti-Money-Laundering (AML) systems can respect privacy. Argumentation, observation and evidence synthesis are the main modes of inquiry for this work. The roles of these modes of inquiry are described below. For a more elaborate description of thought process behind the methodology, see Appendix A. The dynamics are also schematically displayed in Figure **??**.

1.3.1. Argumentation and Conceptualisation

Because "privacy-friendly AML" is as much an ethical question as a technical one, the research begins with a description of how privacy in AML/CFT is perceived from an ethical perspective. Based on privacy theory and expert opinion, the study builds a framework that specifies which monitoring practices come with which privacy impact. This argumentative step is the project's first deliverable.

1.3.2. Observation

To ground the framework in practice, semi-structured interviews are held with AML analysts, regulators and privacy scholars. Questions centred on current data flows, analytic techniques and plausible future

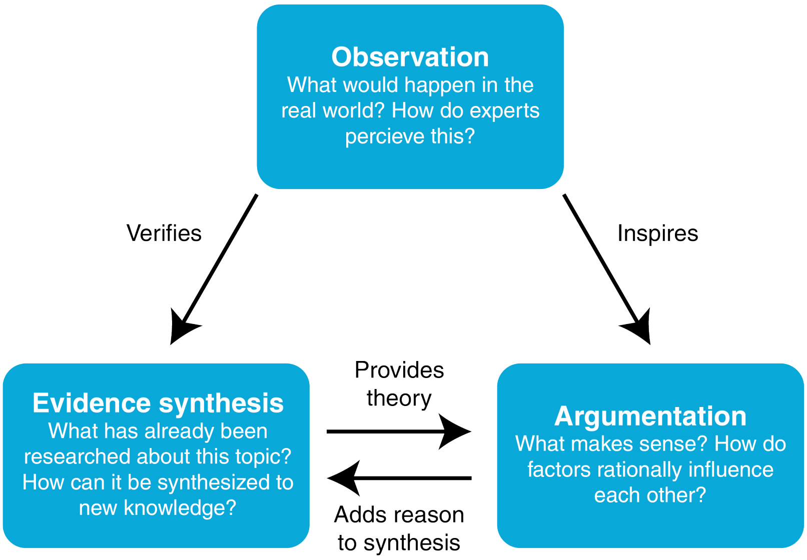
Observation
What would happen in the real world? How do experts percieve this?
Verifies
Inspires
Evidence synthesis
What has already been researched about this topic? How can it be synthesized to new knowledge?
Provides theory
Adds reason to synthesis
Argumentation
What makes sense? How do factors rationally influence each other?

Figure 1.3: The relation of the three modes of inquiry

scenarios.

1.3.3. Evidence Synthesis

Existing reports and expert interviews will be used to compare the framework to the real world refine the argument. Combining these sources with the framework creates a more direct application to the real world.

2
State of the art

This chapter will cover the state of the art when it comes to research about privacy in AML/CFT. The chapter will create a context for the knowledge gaps defined in chapter 3. As stated in chapter 1, privacy is influential in the AML/CFT field, but it is still poorly defined in the context of detecting Financial Economic Crime (FEC). This literature review will look into some of the research that has already been executed on AML/CFT and its relation to privacy. This will be done by first looking at the current AML/CFT approach. After that, some typical privacy considerations will be enlightened. The last section will be a description of techniques currently in development to bridge these considerations and why they can not be implemented effectively yet. This chapter will look into the theoretical and social dimension of privacy briefly, a more thorough ethical privacy analysis takes place in chapter 5.

2.1. Assessment of the current AML/CFT approach

2.1.1. Banks as gatekeepers

Banks are used to execute digital transactions or withdraw and deposit cash. This is convenient when an individual wants to transfer money to a friend, do groceries with a debit card or pay rent. Unfortunately this convenience also applies for less innocent activities which makes bank a primary tool for FEC. Governments are aware of this, that is why banks are given a key responsibility in the fight against FEC. When banks take insufficient measures to prevent or detect FEC, they can even be held responsible for the money laundering that occurs through their platforms. The banks position in this system is often referred to as a gatekeeper role.

There are many critical sounds towards the AML/CFT strategy that is being applied right now. According to Pol (2020) the current system has high compliance cost, but intercepts only a negligible fraction (approximately 0.1%) of illicit cash flows. This could be an indicator that current anti-money laundering policy is ineffective and maybe even useless, which suggests the need for structural reform in AML design and execution.

However, even when factually true, the cited 0.1% figure needs a fair share of nuance when it comes to determining the effectiveness of AML/CFT policies. It measures only funds intercepted and does not factor in the money that has not been laundered because of AML policy. Gerbrands (2022) provides a more nuanced perspective by using a network analysis informed by interviews with criminals. This research showed that the 2015[1] AML policy changes in the Netherlands *did* make laundering more difficult: The implementation of this research caused criminals to need to specialize in money laundering or collaborate with a third party that is specialized in money laundering. The conclusion of this research was therefore, that the Dutch AML policy can be seen as effective. While the total percentage of seized funds remains small, AML requirements do raise barriers that complicate criminal operations.

Both Pol (2020) and Gebrands (2022) conducted factually correct research, but their conclusions are

[1] According to Gerbrands, the effectiveness of an AML/CFT policy can only be assessed when sufficient information is known from registered convictions. This is the reason that the paper could not asses any policies from later than 2015

completely different, this has to do with expectations the authors have of a 'good' money laundering strategy. If the goal of an AML policy is to eliminate every instance of money laundering, the current system seems almost useless. However, if the objective is to discourage criminals by making money laundering sufficiently difficult, then the same system may be considered more successful.

2.1.2. Practical limitations

In the Netherlands around 6 billion digital transactions are executed every year (Betaalvereniging Nederland, 2025), this means that systematic and automatic analysis of transactions is required to effectively assess all transactions on their FEC risk. Transactions that are reported as 'suspicious' by these models are not always connected to money laundering, or can even easily be explained when looking at the data a bit more thorough. These so-called false positives are a big problem in transaction monitoring. Currently, the amount of false positives in AML models is over 90% (Ketenci et al., 2021). This means that 90% of the transactions that are investigated do not contribute to the detection of money laundering behaviour. Unnecessary investigation of individuals' behaviour is an inefficiency that leads to high costs. On top of that, this large amount of false positives comes with major privacy issues.
A contributor to the high amount of false positives is the rule-based structure of typical AML models. This means that the alerts go off based on objective indicators such as high transaction amounts, unusual frequencies or sudden location changes. Rule-based models are transparent in how certain transactions are flagged—after all, every flagged transaction has a clear indicator. However, they often fail to grasp the nuances of transactional behaviour (Oztas et al., 2024).

Traditional AML systems rely mostly on rule-based triggers that analyse each transaction as suspicious or not. While these can catch straightforward anomalies such as an unusually large transaction from a low-balance account, they frequently miss more sophisticated laundering patterns. Jensen and Losfidis (2023) argue that advanced statistical models and machine learning techniques can detect subtle patterns that rule-based systems might overlook, particularly if they can access richer contextual data on each user. While promising, artificial intelligence also brings privacy risks. That is why implementation comes with controversies regarding reliability and privacy.

Banks only analyse transactions that are made through their own services. This gives a shallow perspective on customer behaviour. Money launderers use this lack of insight for individual banks by spreading their transactions across several accounts or banks. These sophisticated money laundering schemes let money travel around the world an average of five times before placing it in their definite resting place (Ferwerda et al., 2020). Transaction monitoring from the perspective of a single bank misses out on patterns like these which makes them miss out on a lot of information.

When data is isolated within each institution, AML/CFT monitoring has a limited view of user behaviour. By contrast, if banks share transactional and customer data, they can collectively identify patterns that might appear suspicious when examined in isolation. Bociga et al. (2024) notes that cross-institutional data sharing allows for more accurate risk assessments and earlier detection of complex laundering schemes. Collaborative AML initiatives also promote resource sharing, reducing compliance costs for individual institutions. For smaller banks especially, sharing data can provide a bigger piece of the picture that would otherwise be nearly impossible to address independently. Moreover, information shared about emerging threats, such as new laundering typologies, can help all participating institutions update their detection models more quickly, thus maintaining a collective defence posture. Centralizing user data also raises cybersecurity concerns, as a single large database becomes a lucrative target for cyber criminals. Labib et al. (2020) warns that a breach in such a centralized system would not only compromise individual privacy but also risk global financial stability.

On top of a lack of cooperation between banks, the AML/CFT system could also benefit from increased cooperation between banks and governments. Banks have a lot of data to their availability and governments have the resources to take forensic action on criminals. PPP's are considered as a key feature of the AML/CFT system, as more collaboration between banks and governments would allow for faster detection of criminals (KPMG Advisory N.V., 2024). PPP's could have several shapes and forms, all differently effective. A form of PPP that is relevant from the perspective of false positives is suggested by the Dutch banking association in 2024 (Nederlandse Vereniging van Banken, 2024). This form allows banks and government to operate based on priorities set together with the government and use national coordination to tackle these problems. This means that the strategic part of the flagging obligation of banks is taken away from them.

However, while PPPs can significantly improve effectiveness in money laundering detection, they also raise major concerns related to privacy and data protection. Sharing sensitive financial data between banks and governmental authorities introduces complex legal and ethical challenges. These partnerships often require the exchange of personally identifiable information, which may conflict with GDPR regulations, especially when the legal basis for sharing is not clearly established. The fear of legal repercussions or reputational damage makes many institutions hesitant to fully engage in PPPs. As a result, promising collaborative structures are often underused or delayed in implementation due to the lack of clear regulatory frameworks and the tension between operational efficiency and individual privacy rights.

2.2. The conflict between transaction monitoring and privacy

The developments described in the previous section are all facing privacy obstacles in their implementation. But what do these privacy objections actually mean? Solove (2009) argues that privacy is not a single principle but rather a constellation of related issues arising from diverse information-gathering and handling practices. This statement resonates with Friedewald et al.(2013), which follows Clarke (1997) in outlining multiple dimensions of privacy, such as the privacy of data, communications and behaviour.

This complexity is also present in an AML/CFT context: Information that is concerning someone financial status such as bank account balance or salary is sensitive but so is information that is connected to a bank account such as a name, address or social security number. Financial transactions can also display sensitive behaviour: a donation to a political party or charity can indicate political orientation and consistent high cash withdrawals near a casino can indicate a gambling addiction. The sensitivity of financial data calls for a careful approach to where, and how this data can be processed. chapter 5 will go deeper into the exact types of privacy that are relevant in transaction monitoring and specifies on how transaction monitoring is harmful to privacy as a concept.

Within the European Union, the General Data Protection Regulation (GDPR) sets strict standards for personal data handling. Transaction monitoring is also covered in the GDPR. recital 4 for example states that data-protection should be in balance with other fundamental rights. Similarly, the EU Charter of Fundamental Rights, Article 8, asserts that data must be processed fairly, with clear consent and under independent oversight. While these regulations aim to protect individuals from invasive data practices, they can also hinder banks from effectively sharing information or constructing detailed user profiles. Even anonymized or pseudonymized data may be considered personal if it can be re-linked to an individual, further complicating compliance. The privacy tensions between different EU laws are elaborated on in 4

Privacy concerns extend beyond regulatory compliance. Institutions that handle vast amounts of personal and financial data face reputational damage and legal liability if they mishandle it. Stallings 2024 warns that transaction datasets can reveal sensitive aspects of someone's life. This goes from daily routines to political or religious affiliations. A breach of such data could irrevocably undermine public trust, thereby eroding the legitimacy of financial institutions and the wider AML apparatus. Thus, even well-intentioned AML initiatives risk reputational harm if they fail to adequately safeguard personal information.

The modern world already subjects individuals to extensive surveillance through : street cameras, smartphone location tracking and browser cookies that create detailed consumer profiles. While some might argue that privacy is "already lost" (Holtzman, 2006), financial data remains uniquely revealing. An individual's spending patterns can expose highly personal details. They can expose political donations, medical treatments, gambling habits or intimate relationships. Stallings (2024) therefore classifies payment data among the most sensitive of personal information.

Yet the very qualities that make financial data sensitive also make it attractive for anti-money-laundering (AML) efforts: detailed records help trace illicit funds and safeguard the integrity of the financial system. This creates a structural tension: stronger surveillance leads to a safer world, but it comes with massive damage on privacy. Despite this dilemma, there is surprisingly little research on how to preserve financial privacy *within* AML frameworks. Exploring that gap is therefore a key challenge for the remainder of this thesis.

2.2.1. Privacy-preserving techniques in AML collaboration

The privacy objections to AML practices are well known. That is why techniques are being developed that ensure privacy in collaboration. Some key techniques are highlighted below.

Federated learning

Suzumura et al. 2022 highlights *federated learning*, which enables machine learning models to train on distributed data without requiring the raw data to be shared. This decentralised approach can boost AML effectiveness by up to 20%, allowing institutions to benefit from each other's data without revealing sensitive information. While federated learning can theoretically boost an algorithm's performance, there are several reasons why simply implementing this technique does not fully solve the AML/CFT problem. First of all, federated learning means that only training parameters are exchanged between separate models. When only training parameters are exchanged, it is not possible to identify FEC that occurs across multiple banks. Also, it is not possible to track the outcomes of federated learning to a specific user. This makes it barely an improvement for forensic research, where concrete, user-specific evidence is often required.

Differential privacy

Differential privacy is another privacy-preserving technique that has experienced fast growth. The central objective of differential privacy is to render each data point non-discriminatory while upholding specific statistical attributes required for data analysis (C. Xu et al., 2023). This is done by introducing calibrated noise into the dataset, which makes it harder to identify loose data-points in data sharing. As a result, it allows for more privacy-friendly data collaboration between institutions.

While both techniques described above have a theoretical benefit to model effectiveness, their implementation is dependent on how data is stored and exchanged. More importantly, these solutions do not solve the deeper dilemma: transaction monitoring is inherently a privacy violation. No matter how well privacy is technically preserved during collaboration or model training, the practice still involves large-scale observation of personal financial behaviour. Therefore, the solution to this dilemma is less a matter of technological optimisation, and more a matter of *defining the ethical and legal values* that underpin such surveillance.

2.3. Conclusion

Banks are stuck between high AML compliance costs and thorough inspection from regulators. On the other hand, the tools that promise the biggest improvements bring the greatest privacy concerns. Due to these conflicting pressures, banks are currently forced into a less efficient strategy: using a lot of manpower.

This is expensive and ineffective in the long term. Scholars stress that robust, scalable AML solutions require a delicate balance between advanced analytics and preserving financial privacy. While technical solutions such as differential privacy and federated learning offer partial improvements, they do not address the core question of how much privacy sacrifice is acceptable in the name of financial security. The implementation of these techniques must therefore go hand in hand with a deeper understanding of the role privacy plays in transaction monitoring.

To move forward, privacy should not be perceived as a barrier to innovation, but as a network of connected risks and obligations that must be critically examined. A better understanding of privacy can not only lead to a more privacy-friendly AML system, it can also improve efficiency. After all, privacy and efficiency share the same goal: inspecting exactly the right amount of people, at the exact right level of depth. This perception is the first step toward a situation in which privacy and effectiveness go hand in hand.

Ultimately, this calls for more thorough research into privacy in AML, not only from a technological perspective, but also from legal, ethical, and social viewpoints. Only with this holistic approach can the AML/CFT system become both effective and just.

3 Knowledge gaps and research questions

The literature review in chapter 2 revealed that a better understanding of privacy in transaction monitoring is necessary. There is a lot of theoretical research about privacy. Still, privacy in an AML/CFT context is poorly defined. As stated in Solove (2009) privacy is a broad, deep and undefined concept. Also, privacy is depending on context and the values of individuals. This means that a specification on the contextual privacy dynamics is required to asses future developments on their impact to privacy.

The goal of this research is to generate knowledge that can contribute to the navigation of the dilemma between privacy and effectiveness of AML/CFT protocols. This will be done by breaking down the concept of privacy and looking into the dynamics between different parts of privacy and how transaction monitoring changes these dynamics. This will lead to a better understanding of the meaning of privacy and therefore to clarity in how the AML/CFT policy should consider privacy. This goal can be achieved by answering the following research question.

> RQ: How can privacy impact be systematically assessed and proportionately balanced against effectiveness in AML/CFT within the Dutch banking sector?

This research question is broken down into the following knowledge gaps, which will be answered with their own sub question.

3.1. Tension fields between privacy and AML/CFT laws

Gap: The European General Data Protection Regulation (GDPR) is considered the worlds most thorough data protection law (Bakare et al., 2024), but even the GDPR leaves room for interpretation. On the other hand there are money laundering specific laws such as the Dutch anti money laundering law (Wwft) and the European Anti Money Laundering Regulation (AMLR). While knowledge about all these laws is publicly available, it requires synthesis to be translated to policy requirements.
Implications: Tension fields in laws are normal and not a problem by themselves. What makes the situation of AML/CFT unique is that the tension is not only in the laws, but also in the values these laws represent. In this specific situation where millions, or even billions of transactions are monitored based on an interpretation of these ambiguities, a misinterpretation of privacy laws can lead to a systematic neglect of privacy.
Research: Chapter 4 will investigate the tension between the laws concerning AML and privacy. These laws are: the Dutch anti-money laundering law(Wwft), the EU General Data Protection Regulation(GDPR) and the new EU Anti-Money laundering Regulation(AMLR). The analysis of the laws shows the tensions between the laws and where AML/CFT purposes can overrule privacy laws, or vice versa.
Research question: Which tensions arise when the GDPR, Wwft and AMLR are applied simultaneously to AML/CFT and how do these tensions shape the legal dimension of AML/CFT operations?

Deliverable: This research will look into the EU laws and find tension fields between them. This will sketch the obligations banks have in combatting financial economic crime and the tools they are allowed to use for this.

3.2. Specifying on the privacy impact of AML/CFT

Gap: Since transaction monitoring collects and analyses user data in a systematic way, it is inherently a privacy risk. Still it can be ethical to do if the societal benefits weigh up against the privacy harms. In order to do this, the proportionality of privacy harms have to be defined.
Implication: The privacy laws discussed in chapter 4 leave room for interpretation. This means that the laws fail to capture the exact balance between safety and privacy which in turn leads to a risk of systematically under- or over estimating the importance of privacy.
Research: Chapter 5 will look the details of the role of privacy in AML. This will first be done by looking at some established works on privacy. These works will be adjusted and applied to the context of AML/CFT after which concrete privacy harms of transaction monitoring can be identified. After that the dynamic between these harms will be enlightened.
Research question: How is the impact of AML/CFT on financial privacy defined?
Deliverable: Detailed overview of the impact transaction monitoring that can be used to asses future developments on their impact to privacy.

3.3. Privacy impact assessment of developments in AML/CFT

Gap: While many technical and institutional developments in AML/CFT are presented as efficiency improvements, their privacy implications are rarely evaluated in a systematic and comparative manner. Existing assessments often treat privacy as a legal obstacle or afterthought, rather than as a central design concern.
Implication: This lack of understanding of the privacy impact of an implication might lead to privacy violations when implemented, or unnecessary development obstacles when not implemented
Research: Chapter 6 will apply the framework from chapter 5 to the developments identified in chapter 2.
Research question: How do key developments in AML/CFT such as AI, data sharing and public-private partnerships, influence the privacy impact of AML/CFT operations?
Deliverable: Privacy impact assessment of key developments in AML/CFT.

3.4. Policy design for proportionate AML/CFT

Gap: There is no widely accepted set of design principles or governance strategies for balancing privacy with effectiveness in AML/CFT systems. While laws such as the GDPR refer to proportionality and data minimization, these principles remain vague and are not consistently operationalized in the financial crime context.
Implication: Without clear design guidelines, banks and regulators may over-rely on technical compliance or apply inconsistent criteria when implementing transaction monitoring, data sharing, and AI-based systems. This may result in either ineffective surveillance or unnecessary privacy violations.
Research: Chapter 7 (Policy design) will synthesize the findings from the legal analysis, harm categorization, and impact assessments to propose normative design strategies that can guide banks and regulators in developing proportionate AML/CFT policies.
Research question: Which design principles or governance strategies can help ensure proportionate AML/CFT practices in the Dutch banking sector? **Deliverable:** Policy design recommendation for proportionate AML/CFT implementation. these recommendations can inform decision-makers on how to balance privacy and AML/CFT effectiveness.

4 Analysis of the laws concerning privacy in AML/CFT

4.1. Introduction

As stated in chapter 2, banks operating within the European Economic Area (EEA) must comply with local Anti-Money Laundering and Countering the financing of Terrorism (AML/CFT) requirements, this requires analysis of their customer data. When analysing this data, banks have to respect privacy rights as well. This means that there are limitations on the techniques that banks can use to comply to AML/CFT requirements.

This chapter provides an overview of the most relevant laws that shape the legal playing field that banks have: the General Data Protection Regulation (GDPR), the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft) and the European Anti-Money Laundering Regulation (AMLR). Throughout this chapter, the tensions between these laws in the field of AML are exposed. This chapter will focus on answering the sub-question:

> Which tensions arise when the GDPR, Wwft and AMLR are applied simultaneously to transaction monitoring for identifying financial economic crime and how do these conflicts shape the legal dimension of AML/CFT operations?

4.1.1. Privacy and data protection

Before the analysis of the laws start, a distinction has to be made between privacy and data protection. Privacy and data protection are different, yet strongly connected, both are considered as fundamental for democracy and are covered in EU law. Privacy refers to the right of a private life and individual autonomy, while data protection considers fair and lawful processing of personal information. The EU charter of fundamental rights covers both concepts and the GDPR focusses on the practical application of data-protection (European Data Protection Supervisor, 2025).

It is important to realize this difference. Data protection is a part of privacy, and protecting data is a good effort towards protecting privacy. However, there are societal concepts of privacy that cannot be captured in a threshold.

In an AML/CFT context, data-protection can be seen as a way to enforce privacy, but not guarantee it. Privacy has a philosophical and value based nature which means that it is extremely hard to express in specific rules (D. Solove, 2009). Therefore, this chapter will mostly focus about the technical, data-protection related laws. The philosophical aspect of privacy will be covered extensively in chapter 5.

4.2. The General Data Protection Regulation (GDPR)

The GDPR, introduced in 2016, harmonizes data protection laws across the EU and EEA. It is internationally acknowledged as the most rigorous data-protection law (Buckley et al., 2024) and is considered to be far stricter than for example US privacy laws (Bakare et al., 2024). The GDPR applies to every process in which personal data is processed which makes it relevant to the field of transaction monitoring. The GDPRs most relevant articles are:

4.2.1. Article 5 - Principles relating to processing of personal data

This article is relevant because these principles form the foundation of data protection and create the most fundamental tensions with AML/CFT practices.

- **Article 5(b)** is about *purpose limitation*. This states that data must be collected for specified, explicit and legitimate purposes and not processed in ways incompatible with those purposes. This is crucial because banks collect transaction data primarily for payment processing, but AML/CFT requires analysing this same data for crime detection. The article states that data should be collected for specified, explicit and legitimate purposes and not further processed in a matter that is incompatible with this purpose.
- **Article 5(c)** states that personal data should be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This concept is referred to as *data minimization*. In an AML/CFT context it is hard to identify which data is necessary for the purpose of exposing money laundering. As technology advances, money launderers have more access to sophisticated techniques, this means that exposing money laundering will be more and more about details. This makes the border of which data is deemed 'necessary' increasingly vague.

4.2.2. Article 6 - Lawfulness of processing

Article 6 is relevant because it determines the legal foundation for all AML-related data processing. This makes it a key article in defining the legal playing field of the banks gatekeeper position. Two sub-articles are particularly relevant in an AML/CFT context:

- **Article 6(c)** states that processing is lawful if it is deemed *necessary for compliance with a legal obligation* to which the controller is subject. In the context of AML this article stresses the thin line banks are balancing. On the one side they have the legal obligation to respect their users privacy, on the other hand they have to comply to a legal obligation which makes it necessary to analyse their users data.
- **Article 6(f)** states that processing is lawful when it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This leaves room for interpretation as it is unknown how privacy weighs against the detection of money laundering.

4.2.3. Article 12 - Transparent information communication and modalities for the exercise of the rights of the data subject

Financial institutions are required to inform customers about how- and why their data is being collected and used. This involves providing clear and accessible privacy notices, including the purpose and scope of data processing for AML/CFT compliance. This part of the GDPR is also delicate since too much transparency will give away to much information about a banks AML/CFT strategy which gives criminals a blueprint to an untraceable money laundering strategy. Banks have to be transparent about how data is processed, but not to the extent where they give away exactly how data is processed.

4.2.4. Article 22 - Automated decision making

This article is relevant because modern AML/CFT systems are dependent on automated flagging systems. The article gives individuals the right to not be subject to decisions based solely on automated processing with legal effects. Translating this to an AML/CFT context, automation is allowed, but when this leads to follow-up actions, it always has to be verified by a human.

4.2.5. Article 25 - data protection by design and by default

This article is relevant because it determines how privacy must be integrated into AML system architecture from the ground op. It states that data protection principles be integrated into all stages of system and process design. This requirement places constraints on large-scale data sharing initiatives, as institutions must ensure minimal privacy risks when implementing AML and transaction monitoring solutions.

4.2.6. Article 35 - Data protection impact assessment

Banks and financial institutions must carry out a Data Protection Impact Assessment (DPIA) when processing activities are likely to result in high risks to the rights and freedoms of individuals. AML/CFT systems employing extensive transaction data analytics typically trigger the need for such an assessment.

On top of these articles there is a general trend where data rights of the subject such as: the right to rectification, right to erasure, right to restriction of processing or the right to be forgotten can be denied when this serves a societal purpose. Transaction monitoring applies this exception as it has the purpose of defeating crime. This means that it is not possible to deny transaction monitoring or demand that banks erase a specific transaction. The concepts of *data-minimization, proportionality* and *legal obligation* are also key when applying the GDPR to an AML/CFT context. Especially since these concepts leave a lot of room for interpretation.

4.3. The Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft)

The Wwft (Wet ter voorkoming van witwassen en financieren van terrorisme) is the Dutch law implementing AML/CFT measures. The selected provisions below represent the core operational requirements that create direct conflicts with GDPR privacy principles:

4.3.1. Article 10 - Outsourcing limitations

This article demonstrates how AML/CFT legal frameworks can create privacy violations through operational constraints. It allows outsourcing of specific customer due diligence tasks but prohibits outsourcing of transaction monitoring activities. It's relevant because it illustrates how AML legal requirements can force privacy-invasive practices. The prohibition on outsourcing monitoring means banks must conduct all transaction surveillance internally, potentially requiring them to build extensive personal data processing infrastructures rather than using specialized, potentially more privacy-protective, third-party services. This restriction contributed to the Transaction Monitoring Netherlands (TMNL) controversy, where attempts to create more efficient, centralized monitoring were deemed illegal, forcing banks to maintain separate, potentially more privacy-invasive, monitoring systems.

4.3.2. Articles 16-20 - Reporting and confidentiality requirements

These articles require banks to identify and report suspicious transactions to the Financial Intelligence Unit (FIU) while maintaining strict confidentiality about their detection methods. They are relevant because they create fundamental conflicts with GDPR transparency requirements (Articles 12-14). Banks must inform customers about data processing but cannot reveal how they detect suspicious activity. This creates an impossible compliance situation: meaningful transparency about AML processing would undermine crime prevention effectiveness, while maintaining secrecy violates privacy principles requiring clear information about automated decision-making processes.

4.3.3. Article 33 - Data retention requirements

This article creates the most direct conflict with GDPR and represents a fundamental tension between crime prevention and privacy. The article mandates retention of customer data and transaction records for five years after the business relationship ends. This directly conflicts with GDPR Article 5(1)(e) (storage limitation). The retention period is not based on individual risk assessment but applies universally, meaning even customers with no suspicious activity have their data retained for potential future investigation. This creates a presumption of suspicion that conflicts with privacy principles of proportionality and necessity.

4.4. EU Anti-Money Laundering Regulation (AMLR)

Adopted in July 2024, the AMLR creates a single EU rulebook that directly applies across member states. The selected provisions below represent the regulation's attempt to harmonize AML requirements while addressing some privacy concerns, though creating new tensions:

Articles 17-19 - Standardized data processing and customer due diligence
These provisions establish uniform customer due diligence rules and standard data fields (Annex I) across all EU member states. They are relevant because standardization creates privacy trade-offs: while uniform rules provide clarity, they eliminate member states' ability to implement more privacy-protective approaches. The standardized data fields (including beneficial ownership information, transaction patterns and risk assessments) become mandatory minimums, potentially preventing institutions from implementing more restrictive data minimization practices. This represents a shift from privacy-by-design flexibility to compliance-by-standardization.

Article 45 - Data retention and erasure framework
This provision confirms the five-year retention period for personal data after customer relationships end, with explicit provisions for anonymization or erasure after this period. It is relevant because it represents the regulation's attempt to address GDPR conflicts, but creates practical implementation challenges. The article requires institutions to build systems that can automatically identify when retention periods expire across different data types and customer relationships. However, it does not address how to handle ongoing investigations or cases where data may be needed beyond the retention period, creating uncertainty about when true erasure can occur.

Article 9 - Integration with GDPR and AI Act
This provision explicitly references GDPR Article 6(1)(c) as the legal basis for AML/CFT processing and treats AI-driven monitoring as high-risk under the AI Act. It's relevant because it represents the regulation's awareness of privacy conflicts but demonstrates the limitations of regulatory coordination. While the article acknowledges that AML/CFT processing must comply with GDPR, it does not provide mechanisms for resolving conflicts between AML effectiveness and privacy protection. The classification of AI-driven AML/CFT as "high-risk" under the AI Act requires additional safeguards (explainability, bias testing, human oversight) that may conflict with the confidentiality requirements of effective money laundering detection.

Article 43 - Restricted Data Sharing Provisions
This provision permits data sharing with third parties only for customers identified as high-risk profiles. It's relevant because it demonstrates a risk-based approach to privacy protection - limiting data sharing to cases where AML/CFT concerns are elevated. However, the article creates new operational challenges: institutions must develop risk assessment systems sophisticated enough to identify "high-risk" customers while ensuring these assessments do not create discriminatory profiling. The provision also raises questions about what can be considered as adequate "high-risk" determination and whether algorithmic risk assessment can be sufficiently accurate and fair to justify differential privacy treatment.

Articles 35-37 - Anti-Money Laundering Authority (AMLA) Data Processing
These provisions establish AMLA's authority to collect, analyze and share financial intelligence data across member states. They are relevant because they represent a fundamental shift toward centralized surveillance that amplifies existing privacy concerns. AMLA will process personal data from multiple national authorities, creating cross-border profiling capabilities that did not previously exist. While the articles include privacy safeguards, they do not address how centralized processing affects individual privacy rights or how data subjects can exercise rights across multiple jurisdictions. The provisions also grant AMLA broad analytical powers that could enable surveillance beyond traditional AML scope.

4.5. Applying the GDPR, Wwft and AMLR to relevant developments in the field.

Ideally the GDPR, Wwft and AMLR complement each other to create privacy respecting AML/CFT policy. While the AML/CFT laws often give context to GDPR concepts such as data-minimization, proportionality and legal obligation, there are some inconsistencies which lead to ambiguity in the law structure. When looking at the AML developments: Data sharing, Artificial Intelligence (AI) and Public Private Partnerships (PPPs) through the lenses of the three laws several inconsistencies are displayed. These inconsistencies are displayed in table 4.1 below:

Development	**GDPR**	**Wwft**	**AMLR**
Data sharing	• Requires purpose limitation (Art. 5(1)(b)) • Data minimisation (Art. 5(1)(c)) • Must have lawful basis (Art. 6)	• Vague on interbank sharing limits • Does not allow the outsourcing of transaction monitoring to third parties(Art. 10)	• Mandates standardised fields (Art. 17–19) • Allows inter-institutional sharing within group structures for high-risk customers. • Retention: 5 years (Art. 45). • Coordination with Data Protection Board recommended.
Use of AI	• Considered high-risk (esp. biometric/financial profiling) • Requires Data Processing Impact Assessment (DPIA) (Art. 35) • Limits automated decision-making (Art. 22)	• No explicit mention of AI • No guidance on profiling or explainability	• Indirect reference: AI systems must align with AI Act • Encourages technology-neutral risk-based approach • Governance measures align with GDPR's Art. 35
PPPs	• Joint controllership risks (Art. 26) • Outsourcing rules (Art. 28)	• Allows cooperation with government bodies and FIU • No clear rules for data protection within PPPs • Financial institutions remain responsible for compliance	• Encourages national PPPs for AML (Art. 51–52) • Stresses alignment with GDPR • Suggests legal frameworks for trusted PPP cooperation

Table 4.1: Legal positions of GDPR, Wwft, and AMLR on three key AML developments

4.6. Conclusion

The goal of this chapter was to sketch the legal playing field Dutch banks must navigate when monitoring transactions for signs of FEC and answer sub-question:

> Which tensions arise when the GDPR, Wwft and AMLR are applied simultaneously to transaction monitoring for identifying Financial Economic Crime and how do these conflicts shape the legal dimension of AML/CFT operations?

The societal benefit of transaction monitoring overrules several concepts of the GDPR. Some of them are clear but three key concepts of the GDPR are poorly defined in transaction monitoring and are therefore put under tension.

First, *proportionality* demands that any interference with fundamental rights be strictly necessary and balanced against the aim pursued. In practice, however, AML rules impose a broad duty to screen large volumes of data, often without a tailored assessment of individual risk. As a result, banks frequently process more data, for longer, than the GDPR would ordinarily allow. This structural imbalance places the burden of proof on the institution to show why expansive surveillance remains proportional to the threat, even as the threat itself evolves.

Secondly, *data-minimisation* (GDPR Art. 5(1)(c)) requires that only data strictly needed for a defined purpose be collected and stored. The Wwft and AMLR, by contrast, oblige banks to retain transaction histories for at least five years. Because money-laundering techniques grow more sophisticated, it can be argued that "everything might be relevant later," blurring the outer limits of what is really essential. The absence of clear thresholds invites both over-collection (to stay on the safe side of AML law) and under-explanation (to avoid tipping off criminals), leaving customers with limited insight into how their data are used.

Thirdly, *legal obligation* (GDPR Art. 6(1)(c)) provides the gateway that permits otherwise intrusive processing. It confirms that AML duties override individual consent requirements, but it does not settle how far those duties extend, or how they must coexist with the rights to information, erasure, or restriction. The law therefore gives bank a duty, but no instructions on how to full fill this in a responsible way.

When the three laws are applied to relevant AML/CFT developments: data sharing, AI and PPP some inconsistencies show. The inconsistent treatment of AI creates ambiguity around the legal properties of AI implementation. The GDPR and labels large-scale behavioural profiling as "high-risk," requiring explainability and human oversight. The Wwft, meanwhile, is largely technology-neutral and offers little detail on how these safeguards should be embedded in practice. These ambiguities ask for a clearer definition of privacy which is covered in chapter 5

5 Privacy

As concluded from the state of the art in chapter 2, privacy forms a big obstacle in the implementation of technological and societal developments that can enhance AML/CFT detection. In order to overcome this obstacle, a detailed understanding of privacy is essential. This section will first look into the concept of privacy in general, its importance and why it is so hard to protect. This will be concluded with a focus on financial privacy. This creates an understanding of privacy, which is a great step towards better representation of privacy in the AML/CFT discussion. However, a specification on privacy's meaning in AML/CFT is necessary to Once the general concept of privacy is illustrated, privacy works will be used to properly operationalize it into policy. That is why, to define the concept in a structured way the works of privacy scholars Roger Clarke and Daniel Solove will be used. For more information on these scholars and their works, appendix C can be consulted. The theoretical works are useful to specify and operationalize privacy but lack a clear application to AML/CFT operations. That is why in the final step of this chapter, the theoretical knowledge and the practical knowledge will be combined to create a framework that can be used to asses the proportionality of privacy harms. This will have the purpose of answering sub question 3.2:

> How is the impact of AML/CFT on financial privacy defined?

5.1. Why is privacy important?

Privacy is considered important. US court defines it as: the most fundamental of rights and the right most valued by civilized men. It has been declared: 'Essential to democratic government' or 'necessary for permitting and protecting an autonomous life' (D. Solove, 2009).

As explained in section 4.1.1, privacy is more than just data protection. Data protection is measurable, testable and directly applicable. Privacy on the other hand is a value, it varies per person, or even per situation. It is about control and dependency, the feeling that you are left alone and are in control over who knows what about you. Violations of privacy can lead to a feeling of being watched, which causes discomfort.

An uncomfortable feeling is only the tip of the iceberg when it comes to stating the importance of privacy. Sensitive data in the wrong hands can lead to serious real-world implications. Examples of these 'wrong hands' and their implications are:

- **Cyber criminals**
  If banks or governments would be targeted by a cyberattack, the financial data of millions or even billions of people could be used to extract money from accounts. While this can have immense financial damage, the damage of a privacy violation can go further than just finances. An example of this is the Ashley Madison data breach in which a hack-tivist group called 'The Impact Team' broke into the servers of Ashley Madison, a dating site marketing itself as a tool for extramarital affairs. The hackers stole the account information of over 37 Million people (Cross et al., 2019) . This data was held hostage, not for money, but under the demand of a complete shutdown of the

site. After the company refused, the attackers uploaded more than 60GB of raw user data including names, home addresses, credit card records and even profiles of which customers had paid for removal (Cross et al., 2019). Looking at the data protection issues as described in chapter 4, it might seem like this problem could have been prevented by better data-protection. However, the essence in this problem goes further then just data protection. When The Impact Team dumped the data on the internet, the damage from a data-protection perspective was already done. This by itself did not create any damage to society, the damage came when journalists and criminals unrelated to the impact team got their hands on the data and used it to blackmail or expose people. The fact that once data is exposed, everybody with wrong intentions can use this for their own benefit and the data-subject has no control over this shows that privacy is both a societal and a technical problem.
Cyber criminality brings another privacy related risk: Identity theft. On top of the privacy violations, identity theft brings potential legal/financial consequences for the victim. With a certain set of identifiers such as: name, date of birth or address a criminal can apply for: SIM cards, bank accounts or even loans in name of somebody else. Identity theft is a big problem, between 2015 and 2018 close to 40 million EU citizens had, because of the misuse of personal information, incurred significant personal consequences ranging from debt collection to legal problems (Buhmann et al., 2019).

- **Big tech**
  Platforms such as Facebook, Instagram and TikTok are worth hundreds of billions of dollars while they are free to use. This is because the main stream of income for these platforms is using user data for targeted ads (Ketonen-Oksi et al., 2016). This means that social media platforms financially benefit from looking for the limits of privacy regulations, or sometimes even beyond. This can lead to a thorough analysis, or even influence of the behaviour of individuals. The societal damage this can bring is illustrated in the Cambridge Analytica scandal where personal data from over 87 million Facebook users was used to influence voter behaviour during elections, including the Brexit and the 2016 presidential race (Hinds et al., 2020). The data was collected through a third-party app and was later exploited for political profiling and targeted advertising. This is a perfect example of a situation in which data protection does not equal privacy. Facebook's servers were never hacked, no passwords leaked and all profile data sat behind the platforms normal access controls. Yet the company allowed a psychology-research app to harvest the details of tens of millions of user profiles, which then where later sold to an external firm. Users did not consent to this, they did not even know it was happening. The fact that a poor representation of privacy influenced some of the biggest geopolitical developments of this century show the importance of privacy protection in the private sector.

- **Malicious governments**
  Once big-tech is used unethically to gain power, mass surveillance can become a key tool for maintaining that power. This idea is well captured in Cardinal Richelieu's[1] famous quote: "Give me six lines written by the hand of the most honest man, and I will find something in them which will hang him". History offers many other examples of governments engaging in unethical surveillance. In 1965, the FBI's Counter Intelligence Program (COINTELPRO) targeted domestic groups such as the Ku Klux Klan, the Socialist Workers Party, and the Black Panther Party. While initially framed as a national security effort, the program was later heavily criticized for its discriminatory practices and violations of privacy rights (Federal Bureau of Investigation, 2025). On the other side of the Cold War, East Germany's Ministry for State Security (Stasi) conducted what is now considered the largest mass surveillance operation in modern history. At its peak, it is estimated that there was one informant for every 6.5 civilians (Lichter et al., 2019). The intentions behind Richelieu's authoritarianism, COINTELPRO, and the Stasi's surveillance all reflect a dangerous pattern: when governments gain the tools to monitor their citizens, they often use them in ways that undermine civil liberties. Today, with over 5.5 billion people connected to the internet daily (International Telecommunication Union, 2024) and computing power capable of processing vast amounts of personal data, the potential for abuse is greater than ever. Even in countries like the Netherlands, where trust in government is relatively high, global examples remind us why privacy

[1] Cardinal Richelieu (1585–1642) was a key advisor to French King Louis XIII and is considered one of the first rulers to implement authoritarian measures such as press censorship, civilian surveillance, and restrictions on political expression.

> must be a foundational principle in the organization of any government. Protecting personal data is not just a technical issue, it is a safeguard against the misuse of power.

These examples demonstrate that violations can have tremendous effects that extend far beyond initial data exposure. Whether through cyber attacks that enable widespread fraud, corporate manipulation that undermines democratic processes, or government surveillance that suppresses free speech, the loss of privacy alters power relationships in society. In the context of financial transaction monitoring the same dynamics apply as the extensive data collection required for AML/CFT compliance can potentially create similar vulnerabilities and power imbalances.

5.2. Why is privacy so hard to protect?

All together, it can be stated that the importance of large-scale privacy protection is astronomical. However, this is not reflected in how individuals, organizations, and policy makers act on a daily basis.

Despite its importance, individuals often fail to grasp the large-scale implications of privacy. A common argument made to justify surveillance is the ”nothing to hide” argument, in which an individual justifies large-scale privacy breaches by claiming that if you have nothing to hide, you have nothing to fear. This argument is often accepted due to trust in authority, lack of awareness, or perceived irrelevance (D. Solove, 2025). Accepting this argument would make this whole research unnecessary. If only criminals have something to hide, then mass surveillance would be completely justified, allowing banks and governments to maximize their data collection and processing practices to detect FEC.

However tempting, this common argument could not be further from the truth. There is a big difference between not doing something criminal and not wanting to show something to an unknown person. In today’s digital world, bank transactions can reveal many forms of sensitive or unusual data that are not criminal. A thorough investigation of these would give any individual an uncomfortable feeling, despite their belief that they have ”nothing to hide.”

Beyond this misconception, the concept of privacy itself is vague. When it was first introduced, it was defined as ”the right to be left alone.” However, this definition stems from the 1890s, when the invention of the portable camera was considered a privacy risk due to the fact that one could be photographed at any time (Warren and Brandeis, 1890). Since then, the world has changed drastically. Smartphones, smartwatches, smart homes, and even smart doorbells have become common, and each of these devices systematically collects personal data. This evolution has changed the perspective on privacy so much that it is barely recognizable anymore. This societal shift calls for a redefinition of privacy. Although many efforts have been made, no one has achieved a complete and universally accepted definition yet (D. Solove, 2025). The ambiguity surrounding privacy means its protection is often dependent on data protection laws such as the GDPR. And while the GDPR is widely considered the ”best data protection law in the world” (Ryngaert and Taylor, 2020), it does not succeed in eliminating the risk of privacy violations completely.

Privacy is a concept with massive societal impact and should be cherished throughout society. The difficulty, however, lies in the fact that privacy must be safeguarded by the individuals within that society. While individuals highly value privacy, they rarely act to protect it. This phenomenon is referred to as the *Privacy Paradox*: a situation where individuals’ online behaviour regarding personal information disclosure is inconsistent with their expressed privacy concerns (Norberg et al., 2007). Moreover, individuals are often confronted with immediate rewards in exchange for long-term privacy compromises: using a VPN is a hassle, social media requires data to deliver accurate recommendations, and skipping a behaviour-tracking loyalty card might lead to missing out a 10% discount.

This creates a paradox in privacy protection: while the importance of privacy is immense, the distributed nature of privacy violations makes them difficult to understand at an individual level. The combination of conceptual ambiguity, cognitive biases like the ”nothing to hide” argument, and the inconvenience of privacy-preserving behaviours leads to systematic tension around privacy. The damages in the big picture slowly creep up into an individual’s daily life and are traded for short-term conveniences.

5.3. Financial privacy

The importance and vulnerability of privacy apply to financial privacy as well. Financial transactions create a detailed report of personal life that goes further than just monetary exchanges. A set of payment records can reveal where individuals live, what medications they purchase, which political party they support, their work-sleep schedules or their favourite restaurants. This importance reflects in how financial privacy is perceived in society. Consumers make careful considerations when it comes to sharing their transaction data to third parties (Brits and Jonker, 2023)

While today, nobody thinks twice about having a bank that records all transactions, this was not always the case. While currently bank records are used for many purposes, bank records where originally introduced to intercept illicit cash-flows. This happened when the 1970 bank secrecy act stated that banks are legally obliged to keep transaction records(Anthony, 2024). The bank secrecy act has evolved to laws such as the Wwft that gives banks detailed instructions on how to gather, analyse and store data to identify potential money laundering behaviour.

Banks have the legal obligation to live up to transaction monitoring standards, but it is not clear which data is needed for this, who should be able to access this and how it should be analysed. This lack of concrete requirements in the law leaves a lot of room for interpretation. As mentioned in chapter 4, concepts as data minimization leave room for interpretation. In a context where more data makes a job easier, the concept of data minimization is rarely represented properly.

The Right to Financial Privacy Act of 1978 was enacted to protect civilians from unwarranted surveillance. While the idea was solid, it failed to live up to its purpose due to many exceptions in the law (Anthony, 2024). Privacy is not an absolute right, which means that violations can be justified when performing a task carried out in public interest(McCarthy, 2012). As decreasing Financial Economic Crime(FEC) is a public interest, privacy violations that directly lead to a decrease in FEC can be justified more than privacy violations that do not achieve this. The concept of proportionality in privacy harms is discussed further in section 5.5.

5.4. Types of privacy according to Clarcke (1997) and Friedewald et al. (2013).

Due to the far stretch of the concept privacy, defining privacy in a specific context is hard. Closing the curtains in a house is about privacy, but so is using a VPN when browsing the internet. Considering this, just making statements about privacy, without any specification about its definition could leave too much room for interpretation. Privacy scholar Roger Clarke (1997) made a respected effort to define privacy. This resulted in 4 different types of privacy:

- **Privacy of the Person** can be seen as the integrity of an individual's body. An example of a privacy breach in this category is a compulsory body search at an airport or customs checkpoint (Clarcke, 1997)
- **Privacy of Personal Behaviour** is the freedom to behave without surveillance or interference, especially in private settings. A typical example of a situation in which this privacy is at stake is when your movement is tracked without consent, such as through CCTV surveillance of shoppers in a retail mall (Clarcke, 1997)
- **Privacy of Personal Communications** concerns protection of messages and communication from interception or monitoring. An example of this is telephone tapping and recording of calls by investigators (Clarcke, 1997)
- **Privacy of Personal Data** is about control over how personal information is collected, stored, used or shared. An example of this is credit-bureau databases that aggregate an individual's borrowing and repayment history(Clarcke, 1997).

While this typology might have covered all aspects of privacy when it was written. Since 1997 the world has changed a lot. For example, the 9/11 terrorists attacks have changed perspective on airport checks, changing the definition of bodily privacy. Besides societal changes technology also has changed a lot. Moore's law indicates that computing power doubles every two years. This means that between 1997 and 2025 computing power has increased roughly 16384 times. On top of that the amount and methods of data analysis have increased severely, this allows for more detailed analysis at lower costs.

Friedewald et al., 2013 noticed this change earlier on and expanded on Clarcke, 1997' s definition. The typologies of Friedewald et al., 2013 are:

- **Privacy of the Person** protects the bodily integrity of individuals. An example of this is : whole-body imaging scanners in airports that display passengers' naked bodies and even medical conditions (Friedewald et al., 2013).
- **Privacy of Behaviour and Action** concerns the freedom to act without systematic observation or recording. An example of this is unmanned aircraft systems (drones) covertly filming people in public, creating a "chilling effect" on how they behave (Friedewald et al., 2013).
- **Privacy of Communication** aims to keep messages—whether spoken, written or neural—free from interception. An example of this is interception of the data stream between a brain–computer interface (BCI) user and the software, effectively wire-tapping neural signals (Friedewald et al., 2013).
- **Privacy of Data and Image** is about controlling personal data and visual recordings. An example of this is RFID-enabled e-passports whose embedded chip can be read without authorisation, exposing stored biometric images and personal details (Friedewald et al., 2013).
- **Privacy of Thoughts and Feelings** protects mental states from unwanted revelation or manipulation. An example of this are: sensor or BCI systems that read brain activity or stress levels in public to flag "suspicious" emotions (Friedewald et al., 2013).
- **Privacy of Location and Space** is the right to move or dwell somewhere without being tracked. An example of this is Oyster-style RFID travel cards that log every journey, enabling authorities to reconstruct a person's movements. (Friedewald et al., 2013).
- **Privacy of Association** safeguards the ability to meet or identify with others without surveillance. An example of this is drones equipped with cameras and facial recognition hovering over a protest to map who is associating with which group (Friedewald et al., 2013).

The examples Friedewald (2013) uses are more recent and more applicable to the world we live in today. But even this revision is already 12 years old. Computing power and data-collection have increased even more and techniques such as Artificial Intelligence have found its way into society. The percentage of online transactions has increased from 48% in 2012 to over 75% in 2023 (Centraal Bureau voor de Statistiek, 2023). Societal changes, and a specification on the context of AML incentivize a revaluation of Friedewald (2013). Just as changes in the world inspired Friedewald (2013) to revaluate Clarcke (1997).

While almost all of Friedewald's (2013) types of privacy have at least a bit of relevance in an AML/CFT context, not every type of privacy should be considered equally important. That is why the seven types where narrowed down to four. The choice for these four types of privacy does not mean that the other three types are completely irrelevant. For example: privacy of thoughts and feelings can indirectly be violated through financial data as well. When a bank account has low or negative funds, this can be an indicator that this person is stressed. Privacy of the body can also be breached when financial transactions give away details about medical specifications. However these types of privacy breaches are specific to individuals and have little overlap with the anti-money laundering. Which makes them less relevant in the further steps of this research. The key types of privacy in AML are:

- **Privacy of behaviour** is relevant in an AML context. The whole concept an AML model is trying to evaluate is money laundering, which reflects specific behaviour. This means that privacy of behaviour is at stake in transaction monitoring. Ideally only behaviour that is an indicator of potential FEC should be investigated. However, this is very hard, if not impossible.
- **Privacy of association** is represented in the dilemmas that policy makers and banks face. Backwards induction from convicted criminals is seen as the key to better AML Nederlandse Vereniging van Banken, 2024. This strategy is likely to contain a graph based model that will work based on associated cash flows. This is something that should be treated with much care since it puts privacy of association at stake.

- **Privacy of association and space privacy** is relevant due to location being an indicator of potential illicit behaviour. A bank account that is used to deposit money in Delft, and 5 minutes later withdraw money in Brazil has a large chance of being flagged by an AML model. This is useful for the legitimate purpose of AML, but tracking the location of citizens should be prevented at all time.
- **Privacy of Data and Image** concerns information such as name, date-of birth or social security number. This is information that the banks have, and can be used to identify a person. The concept of data privacy can be interpreted as overlapping with the previous three. Personal data can indicate behaviour, association and location. Therefore the term 'personal data' is a bit too vague. The terminology from Friedewald et al. 2013 will be slightly readjusted to make it a better fit to transaction monitoring.

Friedewald et al. 2013's types of privacy give a specification on the concept of privacy, but this by itself is not enough to assess the privacy dynamics of transaction monitoring. Privacy definitions can be useful to define implications but as data availability increases, the grey areas between Friedewald et al. 2013's definitions also increase. This means that a systemic application of these definitions will most likely lead to a privacy typology that has too little nuance.

5.5. Privacy harms in transaction monitoring originating from Solove (2006)

Clarke's types of privacy are useful for categorizing the discussion points regarding privacy in transaction monitoring. It showed that in AML/CFT, privacy is mostly about behaviour and sensitive personal data. Still, this categorisation does not translate to concrete policy implementations yet. In order to do this a more concrete display of the implications of privacy violations has to be used. Solove (2006) [2] argues that categorising privacy is too simplistic and that it fails to capture the nuances in privacy's definition. Instead Solove categorizes based on concrete steps in the data chain. The categories he proposes are:

- **Information Collection**
  Concerns activities that gather data about people. The core idea of this harm is that privacy harms begin when data is first captured from- or about a person, either by observing their behaviour or obliging them to reveal information.
- **Information Processing**
  Concerns ways in which already collected data is handled, transformed or used. The core idea of this harm is that even lawfully gathered data can become privacy-threatening when it is combined, analysed, repurposed or left unsecured. Examples of this range from identifying an individual based on its browsing behaviour to denying a person's access to their own data.
- **Information Dissemination**
  Concerns actions that spread or disclose personal data to others. The core concept of this is that privacy is harmed when personal information is shared or spread inaccurately and beyond its original context, which alters how people perceive, or treat this individual. Examples of this are spreading false data, identity theft or blackmail based on sensitive information.
- **Invasion**
  Concerns intrusions into a person's private life or decision making that do not involve collecting or sharing data. The idea behind this is that privacy can be invaded without actually collecting data. This is done when a person's solitude, home or decision-making autonomy is directly influenced.

Solove (2006) specifies on these categories by defining concrete privacy harms for every category. A concise overview of these harms is displayed in table 5.1

[2] Although this work is nearly two decades old, concerns about its relevance in today's digital society are addressed by Solove himself. In his 2025 publication *On Technology and Privacy*, he states that he revised the taxonomy and he is working on a revised version. This version is not fundamentally different from the harms described in his earlier taxonomy, which indicates that they are still relevant

Category	Harm	Manifestation in AML/CFT	Privacy Relevance
Information Collection	Surveillance	Systematic collection of data used to identify AML/CFT transactions.	Mass financial surveillance; proportionality and data-minimization principles apply.
Information Collection	Interrogation	Follow-up message requests for documentary proof (e.g., payslips, invoices) after a suspicious transaction.	Active questioning creates a risk of an individual having to testify against himself; unnecessary data is created which is not in line with data-minimization.
Information Processing	Aggregation	Financial data has to be aggregated to reveal money laundering behaviour	Aggregation can also reveal other behaviour then money laundering; requires strict limits on scope, retention and reuse.
Information Processing	Identification	Identifying the persons linked to FEC behaviour	Bundling anonymized data may lead to re-identification, which undermines prior anonymization efforts.
Information Processing	Insecurity	Large transaction datasets are an attractive target for cyber criminals, high risks of data breaches	Potential breaches ask for good data-protection.
Information Processing	Secondary Use	Payment data gathered for AML/CFT reused for appliances such as: risk scores, Artificial Intelligence models, or vendor tools.	Must remain within AML scope; AML scope has to be defined based on proportionality concept.
Information Processing	Exclusion	No explanation for why somebody is unrightfully under suspicion of money laundering, some exclusion is necessary	A lack of insight in how personal data is processes decreases data control.
Information Dissemination	Breach of Confidentiality	Transaction data used for other purposes than agreed to with the customer	Decreases control of personal data.
Information Dissemination	Distortion	False positives or biased models label innocent customers as high-risk or linked to criminal activity.	Creates reputational harm and service denial; difficult for individuals to correct errors in records.
Information Dissemination	Exposure	Transaction details (medical bills, political donations) shown to large internal analyst pools or external vendors.	Reveals intimate facts that customers expect to stay private.
Information Dissemination	Increased Accessibility	Central AML data storage searchable by thousands of employees, far beyond the original collectors.	Broader internal access increases the risk of misuse
Information Dissemination	Appropriation	Banks monetise aggregated AML datasets by selling "anonymised" insights to third parties.	Commercial gain from personal data captured under regulatory compulsion; customers lose control.
Information Dissemination	Blackmail	Rogue staff threaten to leak suspicious-activity flags unless a customer pays or complies.	Severe personal and financial harm.
Invasion	Intrusion	Unexpected on-site audits or forensic dives into a customer's personal finances triggered by AML/CFT alerts.	Disrupts home or business privacy without new data collection; harassment.
Invasion	Decisional Interference	Automated freezes or forced account closures that block customers from accessing funds or making payments.	Constrains autonomy over one's financial choices

Table 5.1: Solove-taxonomy privacy harms in an AML/CFT context

5.5.1. Categorizing privacy harms by AML relevance

What makes transaction monitoring unique from a privacy perspective, is that transaction monitoring is inherently impactful to privacy. The goal of transaction monitoring is to identify money laundering out of bank transactions. In order to do this banks must capture all transaction data *(surveillance)* analyse this to spot patterns *(aggregation*) and eventually identify criminals *(identification).* Referring to these actions as 'harms' gives them a negative tone which does not reflect the societal benefit they bring.

When it comes to crime detection, privacy should not be used as a shield to hide illegal activities. A speed camera captures a person's location, but only goes of when a certain speed limit is met. When receiving a fine for speeding, it is impossible to invoke a right to location privacy to invalidate the ticket. When a more serious crime is committed, national police might even spread pictures of suspects, or go through suspects phones. While these actions are all harmful according to Soloves (2006) taxonomy, and impact the privacy of these individuals, in the case of crime detection they are not harmful to society.

Translating this to AML/CFT, it can be said that monitoring transactions is inherently harmful to privacy. However, some of Soloves' harms contribute to a safer society to the extend that they are proportionate to the privacy harm they bring. Therefore, from now on this research will deviate from the terminology that Solove uses. The harms as described above are from this point on rephrased to 'impacts' and within these impacts the report will work with three categories:

- **Necessary risks: Information instruments that form the core of transaction monitoring.** These privacy impacts are essential to the functioning of an AML/CFT system. Without them, transaction monitoring would be impossible. When a data collection method is being used solely for the purpose of identifying FEC, and does this with great accuracy, this collection method can be seen as proportional. In the real world this is not the case, that is why these measures are still referred to as risks. They can turn harmful to society once accuracy is lacking.
- **Threats: Privacy harms that can enhance transaction monitoring but are not essential.** These actions are not strictly necessary but can improve detection capabilities. This makes the use of them tempting, but they also bring increased risks of a privacy harm.
- **Harms: Privacy harms that bring no transaction monitoring benefits and have a high risk of occurring.** These harms do not contribute to the detection or prevention of money laundering and should be eliminated or minimized as much as possible.

On top of transaction monitoring being an inherently privacy unfriendly operation, it is also an operation that has clear boundaries. If the goal is to identify money laundering behaviour it can be assumed that actions that do not contribute to this goal are useless from the perspective of banks. This means that once information is acquired through a specific measure, it is no longer necessary to attempt to acquire this information through a different measure.

5.5.2. Necessary risks, Impacts that form the core of transaction monitoring

When defining which privacy impacts are essential for transaction monitoring, first the purpose has to be defined. Banks have the goal to identify, and prevent money laundering through their services. In other words, banks need to apply *surveillance* of transaction data, *aggregate* this to reveal money laundering behaviour and then *identify* the money launderer connected to the behaviour.

Information Collection | Surveillance Surveillance is watching, listening to, or recording an individual's activities. Examples of surveillance are wiretapping or surveillance cameras. Just as with transaction monitoring, these techniques can be useful to detect a suspect. However, surveillance by banks can lead to feelings of anxiety, or even alter behaviour. After all, when a subject has the feeling that he is being watched it is less likely that he will do something that is potentially suspicious. On the other side, the economy has to be shielded from illegal activities, in order to this every transaction has to be recorded, stored and checked. This means that transaction monitoring always needs surveillance of some source.

Information Processing | Aggregation Aggregation is the processing of personal data to make it reveal information. This is relevant in AML/CFT because loose transactions are rarely indicative to FEC.

Individuals that frequently launder money, apply sophisticated strategies to cover up their illegitimate purpose. This means that indications of these types of laundering can only be revealed when data is aggregated to display complex behaviour. When transactions are aggregated to display monitoring behaviour, there can be a big contribution to a safer society. But when it is displaying other behaviour it is an unnecessary invasion of privacy.

Information Processing | Identification Identification is about how well aggregated data can be linked to a natural person. Sanction lists are lists of names of people who are not allowed to make transactions in a specific region. This is something these individuals probably want to evade by using aliases or name adjustments. Also, banks have to link the money laundering behaviour to a specific person, making identification a necessary component of transaction monitoring. These three necessary risks can lead to great societal benefits which makes their harms to privacy proportional. However, this is only the case when they are really contributing to a safer society. Extensive research of a false positive, in which an individual is unrightfully identified as a money launderer, is unproportionately harmful. This means that in an ideal world, *surveillance aggregation* and *identification* only takes place for money launderers. The paradox here is that some analysis is always necessary to know whether an analysis is justified. Where aggregation concerns what can be displayed by analysing data, identification is about how well this can be linked to a natural person. While this seem similar and in the real world they sometimes go hand in hand, they do not necessarily correlate. A bank account of which the data is highly aggregated but fully anonymized, gives a detailed insight to somebody's life without being able to know of which person this insight is given. On the other hand when only direct identifiers such as a social security number, name or date of birth are known, not much about a person's behaviour is known, but there is a strong chance that this individual can be identified. This distinction is important in enhancing privacy. Since transaction monitoring aims to identify money laundering behaviour out of transactions, some sort of aggregation is necessary. However, the step towards identification should only be made when it is known that the person that is being analysed is suspicious. This however, is easier said than done. Aggregation can lead to identification. If behaviour is analysed specific enough, it can be known where a person does groceries, works out, or what his income is. While these transactions may not mean much by themselves, but when insights are combined identification of this individual can occur.

5.5.3. Threats, measures that can enhance transaction monitoring

The purpose of AML data is to determine whether a transaction is indicative of FEC. Once this purpose is served, according to the concepts of *data-minimization* and *proportionality* the data should not be used any more. There is a grey area here where secondary use can enhance future decision making around money laundering. Examples of this are using old transaction monitoring data to train a data-driven algorithm to identify future transaction monitoring. Re-using data outside their original purpose is a privacy harm, but if this serves an underlying social value it might be justified.

Information Collection | Interrogation Interrogation is when information about a certain individual is collected through this same individual. In transaction monitoring the responsibility of interrogation is put in the hands of banks. This makes it that clients can receive phone calls from their bank which asks for clarification on their expense patterns. This makes somebody a witness against himself which is something that goes against the core of many western civilizations. If even suspects in a murder trial have the right to remain silent, this should apply across society as a whole.

Interrogation is something that is sensitive from a privacy perspective. It creates the urge for people to explain themselves. In an AML context banks can be the interrogator when they reach out to a client to ask explanation for an unusual transaction. This is not beneficial for the gatekeeper role banks have and leads to a direct feeling for the user of being watched. Also, the request for an explanation requires subjects to potentially confess to something else which is in conflict with the data minimization concept of the GDPR.

Information Processing | Exclusion Exclusion occurs when a data subject is being shut out of whatever is happening with its personal data. This is impactful due to several reasons. First of all there is a lack of transparency, people cannot verify accuracy or fairness of the way their data is processed.

Exclusion also creates a power asymmetry between banks and their users where banks control which information is reported to the FIUs and users have no say in this.

However exclusion to some degree can be beneficial, or even essential for anti-money laundering purposes. If money launders could easily access the processing policies of banks, that could reveal valuable information about how money laundering can stay undetected. The process of transaction monitoring cannot be publicly available since this would be the golden ticket to laundering money without anybody noticing this.

This creates a tension in AML contexts where complete transparency could undermine the effectiveness of monitoring systems, yet excessive opacity can lead to unfair treatment of legitimate customers and create accountability gaps in the system.

Information Processing | Secondary Use (within AML) The impact is that information is not being used for the purpose that it is intended to be used for. For transaction monitoring this can have multiple outings. First of all there is secondary use *within the context of anti-money laundering*. For example: training a money laundering detection algorithm based on old transaction data. This action is not directly necessary to execute the task of identifying money laundering, but in the long term it can be an enhancer of the process.

information processing, secondary use and *exclusion* are considered as threats because of their temptation for banks. They can make AML/CFT far more effective but also come with losses of privacy. Application of the threats should be done with great care but it can be justified if proportional.

5.5.4. Harms that do not benefit transaction monitoring

On top of the necessary privacy sensitive actions, there are privacy harms that have greater likelihood in AML/CFT but do not bring a lot of benefits. These harms are: *Insecurity, Secondary use (beyond AML), Distortion, Breach of confidentiality, Appropriation, Increased Accessibility, Exposure, Decisional Interference* and *Blackmail*.

Information Processing | Insecurity Insecurity is mostly about data-protection. The impact of insecurity considers failing to protect data against loss or attack. In an AML context the most clear example is when transaction data is breached or leaked. This is not a harm that carries any benefits to detecting money launderers and should therefore be mitigated.

Insecurity is a big risk in transaction monitoring. At the moment over 13 thousand people are working as a KYC analyst in the Netherlands (Nederlandse Vereniging van Banken, 2024), as there are no universal guidelines as to what a KYC analyst can see of a bank user for which person and considering that the false positive rate of flagged transactions is over 90% it can be assumed that there is a risk of personal data, going to places that are not AML related is likely. On top of that there are no official guidelines on how data should be stored, and protected which causes insecurity around whether data is properly secured.

Information Processing | Secondary Use (Beyond AML) Another form of secondary use is when transaction data is used for activities *outside of money laundering*. Examples of this are a system where transaction data is analysed to assess users on their likelihood of paying back a loan (credit scoring) or selling transaction data to external parties for marketing purposes.

Legal transaction monitoring obligation gives banks options to process their data. When this data is used for other purposes such as marketing or a credit scoring system, this would be harmful to the privacy of users. This type of secondary use represents a clear violation of purpose limitation principles, as the data was originally collected under the legal justification of AML compliance but is then repurposed for commercial gain. Such practices can lead to discriminatory outcomes and create unexpected consequences for individuals whose financial behaviour is analysed for purposes they never consented to.

Information Dissemination | Distortion Distortion occurs when inaccurate or misleading information about an individual is created or spread. When a legitimate customer is tagged as high risk, this can give a false representation of him. In the context of AML, distortion can occur through algorithmic bias, false positives in monitoring systems, or incorrect data entry. This is particularly problematic because distortion can lead to reputational damage, restricted access to financial services, and ongoing surveillance of innocent individuals. The automated nature of many AML systems can perpetuate and amplify these distortions, making them difficult for affected individuals to identify and correct.

Information Dissemination | Breach of Confidentiality Breach of confidentiality occurs when data that banks are trusted with is disclosed to someone outside this trust circle. In AML contexts, this can happen when transaction data is shared with FIUs or law enforcement agencies based on suspicious activity reports, especially given the high false positive rates (over 90%) in current monitoring systems. While such sharing is legally mandated, it represents a significant privacy concern when personal financial information about innocent individuals is disclosed to authorities. This breach can have lasting consequences for individuals who may become subject to ongoing investigation or surveillance despite having committed no wrongdoing.

Information Dissemination | Breach of Confidentiality Banks are profit-driven organizations, they use their customers money to hand out loans, invest or give out mortgages. This means that for their core business, banks need their users. Users also need their banks to keep their money safe, Money is necessary for almost everything so the fact that users trust banks with this is worth a lot. When opening a bank account at a specific bank an agreement is made between user and bank, this agreement states that banks use transaction data for legal purposes[3].

5.5.5. What does the categorization of privacy impact tell us?

The categorization of privacy impact creates a strategy to asses the privacy implications of an action. The categorization is shown in figure 5.1.

The core of AML/CFT privacy impact is displayed in the middle circle and are indicated with a green colour, these impacts are essential for AML/CFT and removing any one of them would make transaction monitoring impossible. When evaluating developments in transaction monitoring from a proportionality perspective, a development that increases the harms in the core is likely contributing to a more effective transaction monitoring system. This does not mean that an increase of these impacts is always a good thing. Data can still be *aggregated* to display behaviour that is not related to money laundering,*identification* and *surveillance* of innocent bank users is still an disproportionate action.

One layer to the outside are the harms that are not essential for transaction monitoring, but do have the possibility to increase effectiveness. These are displayed with the colour orange. Harms like these challenge the GDPR concepts of data minimization and legal obligation as explained in chapter 4. For example: *Interrogation* leads to more information, therefore making it easier to identify whether an individual is laundering money, at the same time it is also a massive privacy invasion since people are pressured to explain themselves for behaviour that might be completely unrelated to money laundering. Implementation of these harms requires caution, they are tempting to apply but are not essential to execute the legal task that banks have.

The outside layer are the bullseye are the harms that bring no benefit and are damaging to privacy, these harms are indicated with red. An increase in these harms is brings no AML benefits. For example *insecurity*, there is no sensible policy makers who considers to decrease the security of AML vaults or *Distortion* where the inaccuracy of AML models increases. Despite their lack of nuance, these harms are important for privacy assessments. The harms in this layer are useful as indicators for poor privacy policy. If a development largely brings increases in these harms it is probably a risky move from the perspective of privacy.

5.5.6. Privacy impacts that can exist in multiple layers

Not every impact exist solely in one layer, aggregation to exploit money laundering behaviour is essential but aggregation of behaviour that is not related to money laundering is not beneficial. The same goes for identification, identification of money launderers is beneficial, identification of non-money launderers is not.

[3] The privacy statements of ING, Rabobank, ABN Amro and Volksbank where read to come to this conclusion

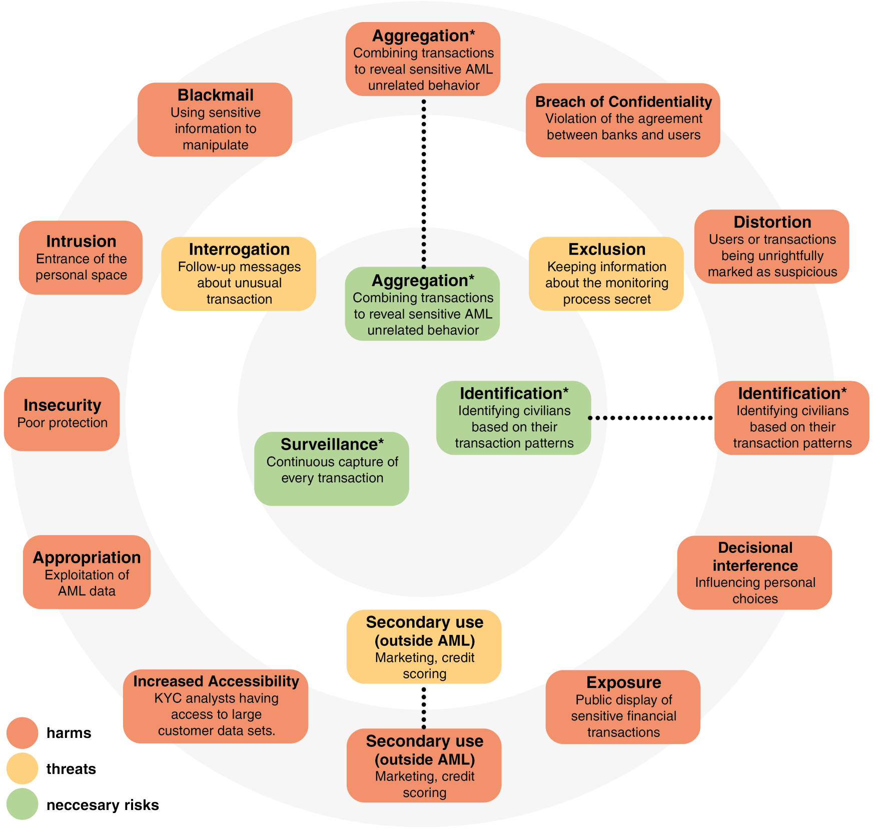
Aggregation*
Combining transactions to reveal sensitive AML unrelated behavior
Blackmail
Using sensitive information to manipulate
Breach of Confidentiality
Violation of the agreement between banks and users
Intrusion
Entrance of the personal space
Interrogation
Follow-up messages about unusual transaction
Aggregation*
Combining transactions to reveal sensitive AML unrelated behavior
Exclusion
Keeping information about the monitoring process secret
Distortion
Users or transactions being unrightfully marked as suspicious
Insecurity
Poor protection
Identification*
Identifying civilians based on their transaction patterns
Identification*
Identifying civilians based on their transaction patterns
Surveillance*
Continuous capture of every transaction
Appropriation
Exploitation of AML data
Decisional interference
Influencing personal choices
Secondary use (outside AML)
Marketing, credit scoring
Increased Accessibility
KYC analysts having access to large customer data sets.
Exposure
Public display of sensitive financial transactions
Secondary use (outside AML)
Marketing, credit scoring
harms
threats
neccesary risks

Figure 5.1: Bulls-eye diagram of the privacy impacts in AML/CFT

Soloves taxonomy inspired a framework that can be used to assess developments on their privacy impact. The statement that drives this framework is that transaction monitoring is inherently privacy unfriendly. First of all, this means that some harms are essential and putting active effort in reducing these harms would mean that the effectiveness of transaction monitoring is directly compromised. In a transaction monitoring context these harms are, *Surveillance* of transactions which are *Aggregated* to reveal behaviour, so that money launderers can be *Identified*. In a perfect systems these impacts would focus solely on money laundering behaviour which means that civilians are mostly left alone. There are actions that can enhance money laundering detection, but bring increased damage to privacy. These threats have to be treated with a lot of care as they are right in the grey area of the lawfulness of processing concept as described in chapter 4. According to the framework, if an increase of one of the core harms can release the risk of another harm, this action can still be privacy friendly. For example, if increased aggregation that leads to a lower need for extra information means that there are fewer follow-up calls, there might actually be an indirect privacy advantage that comes with a direct privacy harm. The last categories are harms that do not have any benefit on crime reduction. Reducing these harms would not lead to any reduction in effectiveness and should therefore be the standard in AML/CFT policy.

On top of that some dynamics between harms can be identified where an increase in one harm, releases pressure on another one. These types of dynamics mean that an action that is harmful in the short term, might actually be beneficial in the long term. Both the categorization and the dynamics between the harms will be essential for composing the requirements of chapter 6 This chapter aimed to define privacy in an AML context. It did not achieve a one-size fits all definition of privacy, and even failed to define it concisely for transaction monitoring. However it succeeded in embracing the complexity of privacy and translating this to something that can be used to assess the effects of innovation on privacy in the transaction monitoring field.

5.6. Conclusion

Both Friedewald (2013) and Solove (2006) take on a different approach to defining privacy. Friedewalds (2013) typology helped to define which types of privacy are relevant in the AML/CFT context, while Solove (2006) provides a breakdown on the ways privacy can be harmed. While both approaches work differently towards defining privacy, they can complement each other in creating a policy advise that is based on a concrete privacy definition. v

Solove (2009) stresses that privacy must be treated not as an individual preference, but as a societal value. However, this value is often too abstract to translate directly into policy. By breaking down privacy into harms, Soloves model makes it easier to design and evaluate AML/CFT measures on their privacy impact.

This chapter had the purpose of answering the sub question

> SQ2: How is the impact of AML/CFT on financial privacy defined?

The most important realization here is that transaction monitoring is inherently harmful to privacy. However, there are differences in whether these harms serve money laundering purposes. If harms that are essential for AML are completely mitigated, anti-money laundering would not work. Also, an increase in these harms can be beneficial for the detection of money launderers. This does not mean that an increase in these harms is always a good thing. *Aggregation* of data that is not AML related is still not justified from the perspective of proportionality. The difficulty here is in the fact that it is only possible to know what data will reveal once it is analysed.

The analysis of the harms is important because it allows for comparison between privacy violations. It helps asses how privacy harms of transaction monitoring weigh up against their societal benefits and therefore contribute to a more proportionate AML policy. The categorization of the harms can lead to various useful insights when it is applied to asses a potential policy. This is done in the next chapter 6

In the next chapter, this framework will be applied to emerging trends in AML/CFT: Artificial Intelligence, data sharing between banks, and Public-Private Partnerships. These developments are often proposed as efficiency-boosting solutions but they come with significant privacy concerns. By systematically assessing the privacy impact of these developments a step towards strucural privacy consideration is made.

6

Privacy impact assessment of key developments in AML/CFT

The law analysis in chapter 4 brought some key tensions and ambiguities in privacy law to light. An ethical filling to these law ambiguities was made in chapter 5. This led to a framework that categorizes the privacy impact of a development on their proportionality to AML/CFT detection. This chapter will apply the defined dynamics of privacy impact to real world developments which leads to a assessment of privacy in the AML/CFT field. To eventually answer research question 3:

> How do key developments in AML/CFT such as AI, data sharing and public-private partnerships, influence the privacy impact of AML/CFT operations?

6.1. General friction points in AML/CFT

The privacy recommendations that will be drafted later in this chapter are applications of the framework to assess the changes in privacy. In order to determine a change, first friction points in the current AML/CFT systems are established. These friction points are influenced in multiple developments and developments can influence multiple friction points. For clarity, the friction points are defined first, and referenced to when the developments are assessed. This allows the assessment of the developments to be all about applying the framework instead of needing to explain the thoughts behind a friction point every time it is brought up.

6.1.1. Over-compliance

Chapter 5 shows that the privacy discussion is about balancing privacy and safety. The framework can be used to assess developments based on their proportionality but this is still missing detail on the safety side of the discussion. Privacy vs AML/CFT is a different discussion than privacy vs safety. In order to give proper insights to the proportionality of privacy violations on AML/CFT, an assessment of the proportionality of anti-money laundering efforts to safety has to be made first.

On top of protecting safety, money laundering controls are macro-economically important. The International Monetary Fund (IMF) warns that unchecked illicit flows "hurt economies" and can trigger financial stability shocks. Yet the IMF states that very little laundered money is ever confiscated, because there is still a major gap between progress on technical compliance and real-world effectiveness. (International Monetary Fund, 2025)

That gap is reflected in the numbers. As shown in chapter 2, Pol (2020) states that less than 0.1% of criminal proceeds are ultimately seized, meaning about 99.9% percent of FEC related transactions can occur without any disturbance, the United Nations' own estimate is almost identical (United Nations Office on Drugs and Crime, 2023). Paradoxically, compliance activity has never been busier.

The Financial Action Task Force (FATF)[1] published a global stock-take report that states that 76% of jurisdictions now meet its 40 Recommendations. This was only 36% in 2012 (Financial Action Task Force, 2022)

Why does more compliance not lead to less crime? A big factor is the way responsibilities are divided. Banks are in a gatekeeper position that obliges them to screen, monitor, filter and report transactions. Because regulators cannot hold banks directly accountable for national crime levels, they judge them on what can be inspected: policies, procedures and paperwork. This shifts banks focus from catching money launderers to technical compliance.

Applying this in the context of the privacy–safety trade-off: if privacy violations are required to comply with an AML/CFT policy, but do not lead to a significant increase in FEC detection, this could indicate that the policy should be reconsidered. While this issue is out-of scope for this research, a takeaway is that a privacy impact that directly enhances societal safety is more proportional than a privacy impact that enhances compliance. Therefore privacy harms for the sake of compliance should be mitigated more than privacy harms that directly contribute to an increase in safety.

6.1.2. Automatic vs manual surveillance

As said in chapter 1, in 2024 over 13 thousand KYC analysts where working in the Netherlands alone (Nederlandse Vereniging van Banken, 2024), the Financial Intelligence Units(FIUs) create approximately 18.000 files with suspicious transactions every year(Netherlands, 2024). Although this seems to imply that each full-time KYC analyst contributes to just over one reportable case annually, this comparison overlooks important nuances. KYC analysts perform a broad range of tasks beyond transaction reporting, including customer onboarding, periodic reviews, and risk assessments. Furthermore, only a fraction of analyst work results in escalation to the FIU, and many suspicious transaction files originate from other sources or involve multiple analysts. Nonetheless, the numbers highlight the scale of manual effort involved in achieving a relatively modest number of investigative leads.

From a utilitarian[2] perspective, the skills and time of KYC analysts can also be used better. The disproportionate amount of KYC analyst is shown when it is compared to the amount of police officers on the streets in the Netherlands, which is around 20 thousand (Ministerie van Justitie en Veiligheid, 2024). This means that there are almost as many people looking through transaction data for financial economic crime as there are actual police officers on the streets looking for criminals. If AML/CFT policy was about safety, these KYC analysts could serve a far better purpose.

One way to increase efficiency is by automating part of the actions that are now dependent on analysts. The question arises if the same amount of surveillance has different harms when it is done by a non-conscious system as opposed to a human being. This section will not yet specify on the technical aspects of this automation, That will be covered a few sections below in subsection 6.2.1.

In some sense systems are more reliable than humans, they execute the task they are assigned, and do only that. Algorithms have no personal interests, cannot be pressured into anything and do not have off days. This means that several impacts of the framework would go down significantly in automation. *Blackmail* from a system would be very unlikely. Automation also reduces the chances of *intrusion* since algorithms will execute the task they are assigned to and do not investigate further than this task requires.

This does not mean that automation comes without privacy risk, algorithms make the same mistake over and over, a systematic, unchecked appliance of these algorithms can lead to more *distortion* or *insecurity*.

Despite a reduction in risks of human vices such as *blackmail*, *interrogation* and *intrusion*, automating a process does not guarantee objectivity. Technology is often seen as an objective factor in our world that completely takes humans out of the loop. However, with complex algorithms this is almost never the case. Humans are responsible for decisions in every step of the design process of an algorithms.

[1] The FATF is a intergovernmental organization that develops and promotes policies to combat money laundering and terrorism financing. FATF established a set of 40 recommendations, which are internationally recognized standards for AML/CFT

[2] Utilitarianism is an ethical theory that holds that the best action is the one that maximizes overall happiness or well-being for the greatest number of people. It focuses on the consequences of actions, judging them as right or wrong based on their outcomes rather than intentions.

Solove (D. Solove, 2025) states that it are humans who decide on the type of analysis, humans that set the training parameters, humans that pick the training data and humans that record the data that is being processed. This means that while technology has the ability to follow a set of instructions and not deviate from it, it is far from objective.

Distortion and *insecurity* risks are lower on simpler applications. Therefore, automation of simple administrative tasks might be beneficial to privacy. As processes get more difficult the risk of *distortion* and *insecurity* increase which means that automation is a bigger harm for privacy as the analysis gets more complicated. This dynamic will be used to assess the impact of AI in section 6.2.1.

6.1.3. Transaction monitoring and transaction filtering.

Prevention and detection of money laundering have different implications in AML/CFT. A measure to prevent FEC is transaction filtering, this is when a transaction is not executed because it possesses a clear threat for money laundering or terrorism financing. Examples of these clear threats are convicted criminals/terrorists that attempt to make a transaction or the trade in so called dual-use goods. Goods that can serve a legitimate purpose but can also be made to use dangerous products such as weapons. From a proportionality perspective there is a clear distinction between analysing and cancelling a transaction.

Transaction monitoring is a form of *surveillance*, every transaction is stored and processed. Usual transactions undergo quick checks and as transactions get more suspicious, processing intensity increases. Once a transaction has reached a point where it is highly suspicious, it gets reported to the FIU. The FIU then investigates this transaction further, adds it to a file and eventually takes the appropriate legal action. In transaction monitoring it is the case that as a transaction is monitored further, privacy impact increases. *Aggregation* increases as analysis gets more thorough. *Identification* occurs depending on the banks pseudonymization policy, but it for sure happens when a transaction is reported to the FIU. Potential *interrogation* might occur if banks cannot find a logical explanation for transactions by themselves. As these impacts increase risks of, *Exposure*(public display of financial transactions) and *Accessibility*(Analysts having access to large customer data sets) increase as well. Depending on values regarding safety and privacy, these increases in privacy harms are justifiable if it leads to important hints of FEC. But these harms are for sure not justifiable if it does not lead to any new FEC-related information. The difficulty in this is that this is a fact that can only be assessed *after* the data has been gathered and analysed.

Considering this it can be stated that decreasing the amount of transactions unrightfully marked as suspicious is therefore very beneficial for reducing the privacy risks of AML/CFT operations. The way to do this is likely by analysing more data and analysing this more thorough. This means that short-term privacy harms can lead to long-term privacy improvements.

Transaction filtering is not about identifying money laundering or terrorism financing behaviour, it is about preventing it. Once an account owner, region, product or transaction amount is linked to a high risk of FEC, banks are required to block transactions from/to this account. The requirements for transaction filtering are more clearly defined: there are publicly available lists of all account holders that are not allowed to execute- or receive a transaction. Lists of prohibited products can be applied directly and high-risk countries are also fairly straightforward. This means that *insecurity* is very low when applying these sanction lists. However, there is always a chance that somebody who is in a high risk country, transporting a high risk good or making a large transaction is doing this for justifiable reasons.

6.2. Developments in the field

The friction points enlightened in the previous section can change through developments. These developments stem from literature, reports and expert information. An elaborate description of how these developments where gathered is in chapter D. The developments are assessed using the framework composed in chapter 5. For every impact from the framework will be defined whether there is a low, moderate or high impact from this specific development. If the impact decreases the effect will be negative and if it is unsure how a impact is influenced this will be indicated with mixed. The privacy assessment is displayed in tabular form.

6.2.1. Artificial Intelligence(AI)

Over the last years AI underwent massive growth, both in research and in patents filed (Maslej et al., 2024). The concept has grown from a niche technology to something that is accessible to everybody with an internet connection. AI is also seen as promising to increase the effectiveness of money laundering. Research has been conducted about the effectiveness of AI based AML models and often, data driven algorithms are indeed better in identifying illicit transactions than rule-based models (Oztas et al., 2024). Common arguments against AI are bias, opacity and dependency on large datasets. Benefits are: fewer false positives, more automation and less need for human oversight. These factors create a complex privacy dynamic that requires thorough analysis. Another contribution of AI is in optimizing the work-flow of documenting. This can lead to more efficient technical compliance which is attractive for banks due to the potential for cheaper, faster and more reliable AML/CFT compliance.

The distinction between these two applications of AI is important because there is a difference in training, and benefits. This means that both the privacy impact and contribution to safety are different. Where analysis of financial data could potentially reveal new money laundering patterns, using AI to speed up compliance would not do this. These two application far from cover all the potential AI has in this sector, however due to time and resource limitations not all applications could be covered in this research. These two applications of AI where chosen for two reasons: These two applications operate close to the financial data of bank users, therefore making them relevant to privacy and these two applications show a lot of potential for increasing societal safety.

AI to make AML/CFT compliance more efficient

At the moment banks have to store and deliver a lot of documents to show that they are compliant to AML/CFT rules. Banks are not only judged on their effectiveness, but also on the registration of their policies. An example of this is that banks have to be able to identify the ultimate beneficial owner (UBO) of every company that is using their services. AI is more than capable in executing this task.

From a privacy perspective, using AI instead of human analysts for these steps generally decreases privacy harms. A system where a large part of the KYC steps are filled in correctly most of the time and only need to be checked by the client requires fewer human attention to the data. Therefore reducing human access to sensitive data, is a low-risk privacy gain. Another advantage of limiting the implication of AI to simple tasks is that the model's training relies only on existing compliance data. This means that there is a limited increase in *aggregation*. The exact description of the privacy impact is displayed in table 6.1

Using AI to reveal complex money laundering patterns Using AI to reveal complex money laundering patterns presents a complex privacy discussion. The potential benefits to society are higher since it can reveal patterns that current methods can not spot. On the other hand, the privacy impact is bigger as well due to increased data collection and opacity.

Accurate AI models needs good, and complete training data. This comes with two risks: First there is the risk of biased algorithms due to poor training data, which results in more people being unrightfully inspected. Secondly, there is a risk in how this data is acquired. If this were to be done by aggregating datasets of multiple banks, a combined dataset would be necessary. A complete dataset like this is undesirable since it means that a national financial data breach is only one cyber attack away. In other words, an increase in training data has a negative direct relation to privacy but this leads to stronger algorithms which decreases unnecessary inspections and therefore is a privacy virtue.

This discussion gets increasingly difficult when the concept of exclusion gets thrown in. An effective AI model needs a lot of data, when this is aggregated it brings risks, but when it is not combined explainability is lacking. The complexity of these dynamics is something that comes back with every application of AI.

A structural assessment of the privacy impact of AI can be done by using the framework defined in 5. This is displayed in table 6.2

Layer	Manifestation in Artificial Intelligence	Effect on privacy	Comment
Core	Limited increase of *surveillance*, only focusses on existing compliance	Low	Uses structured data already collected for compliance purposes
Core	Limited increase of *aggregation*, records are already existing but need to be analysed in a slightly different way	Low	Automates existing workflows without requiring additional data collection
Core	Lower risk of *identification* due to automation	Beneficial	Reduces human analyst access to personal data of bank users
Enhancing	*Secondary use* for AML purposes increases	Moderate	The purpose of this automation is AML related but not directly necessary for the legal flagging obligation
No benefit	*Distortion* decreases if the task that is being replaced is simple	Beneficial	Consistent with the statement that automation of simple tasks reduces privacy harms

Table 6.1: The privacy impact of using AI to speed up KYC

Findings from the framework

The privacy impact assessment reveals a clear distinction between the two AI applications in AML. Automating compliance paperwork presents minimal privacy risk and may even improve privacy protection by reducing human access to sensitive data. In contrast, using AI for complex pattern detection requires a significant increase in privacy harms.

This analysis suggests that automation of simple compliance tasks can be justified from a privacy perspective. The increase of efficiency would mean an indirect contribution to safety, but direct benefits of automating compliance are limited. The deployment of AI for complex pattern detection requires careful consideration as it has a lot of impact on privacy. The severity of privacy harms does not mean that implementation of AI should always be discouraged. If these techniques bring a significant increase in money laundering detection, and therefore leads to a safer society implementation might be justifiable. In order to weigh this, two things are necessary; A more thorough understanding of the benefits of AI implementation and a determination of the societal weights of privacy and safety.

6.2.2. data sharing between banks

data sharing between banks is seen by experts as a key step in identifying complex money laundering patterns (KPMG Advisory N.V., 2024). An example of data sharing in a Dutch context is the TMNL initiative in which 5 banks collectively analysed data of their customers. The thought behind this is that sophisticated money laundering patterns, where transactions are spread across multiple banks can be detected more easily with cooperation between banks. While this initiative seemed like a great step towards detection of complex money laundering patterns, it was unpopular and considered very privacy invasive (Strop, 2024). On top of that the European Anti-Money Laundering Regulation (AMLR) states that data sharing in this form is only allowed for high risk customers. This did not match the intentions of TMNL, since the goal of TMNL was to identify new high-risk users based on their transaction patterns. This meant that in foresight of the AMLR, TMNL had to scale down operations.

From a proportionality perspective, the TMNL use case is interesting. There was a lot of potential but

Layer	**Manifestation in Artificial Intelligence**	**Effect on privacy**	**Comment**
Core	*Surveillance* significantly increases as AI models demand complete transactional data for training	High	Predictive accuracy correlates with data breadth (Q. Xu et al., 2025) limiting input data decreases performance
Core	*Aggregation* severely increases since AI requires extensive data processing	High	AI models need detailed data representing society, this also requires detailed data of good willing citizens
Core	*Identification* decreases through automation but increased data collection	Mixed	Removes humans from decisions but more data is required which increases reidentificaiton risks
Enhancing	*Secondary use* for AML purposes increases	High	Using AI is not necessary to compel to a legal obligation but it can enhance FEC detection
No Benefit	*Distortion* increases due to risk of bias	Mixed	Despite its bias, AI can still be an accuracy improvement compared to rule based systems with a 90% False positive rate Ketenci et al., 2021
No Benefit	*Insecurity* Increases due to potential leaks of training data	High	Even with anonymized training data, reidentification is always a risk

Table 6.2: The influence of using AI to enhance transaction-monitoring models on privacy harms.

also a lot of friction with privacy. Applying the framework created in chapter 5 considers data sharing between banks as displayed in table 6.3.

Findings from the framework

When the framework is applied to data sharing between banks, it becomes clear that this development leads to significant changes in both privacy risks and AML/CFT effectiveness. Instead of each bank having only a fragment of a client's data, an external organization gains access to a much more complete dataset that spans all clients. This means that more information about each individual is known, which increases the analytical potential but also the privacy impact.

Identification emerges as a key concern in this setup. Ideally, if the appropriate privacy measures are in place, data is shared in a pseudonymized form with an external party. This party monitors a large transaction dataset and holds the encryption keys that allow individual accounts to be linked across banks. If suspicious behaviour is detected, the relevant data can be de-pseudonymized to reveal the identity of the money launderer. Although the technical specifics of encryption, data collection, and flow management are out of scope for this research, the assumption is that if these safeguards function as intended, the risk of identification remains low.

Insecurity,is the catalyst for more severe privacy harms. Surveillance of pseudonymized individuals is relatively low-risk from a privacy perspective. But the situation changes when pseudonymized data is reidentified without proper cause, or when model inaccuracies result in false positives. In such cases, harms like *distortion* become more prominent.

Overall, data sharing between banks leads to a notable increase in both privacy harms and AML/CFT effectiveness. It expands the pool of data available to analysts, which enhances detection capabilities but also amplifies the risks. The analysis shows that while *surveillance* and *aggregation* increase significantly, the most critical factor for proportionality revolves around the potential for *identification*.

6.2.3. Public private partnerships(PPP)

Over-compliance has a negative impact on both privacy and safety as it harms privacy in exchange for a barely noticeable effect on safety. A possible way to decrease this is by involving government organisations in the transaction monitoring process. This could potentially move a part of the monitoring obligation from banks to governments which would reduce the need for government organizations to check on banks.

The Dutch banking association vouches for national coordination and an increased form of PPP (Nederlandse Vereniging van Banken, 2024). KPMG Advisory N.V. Has also released an elaborate report in which several forms of PPPs are enlightened. This report sees PPP as a route to save costs and improve results of the gatekeeper function (KPMG Advisory N.V., 2023). These results depend on legal clarity and smart governance. The report also identifies the privacy balance as the biggest blockade to successful implementation of PPP. Without a clear political decision on the value of privacy, the ideas stated in this report will never be implemented. This calls for an assessment of the privacy dynamics PPP bring with them.

Civilians have different expectations form banks and governments. Of banks it is expected that financial data and personal funds are kept secure. Governments are trusted with protecting the general safety and wellbeing of society. In PPPs a grey area emerges where banks take on a role in protection society and governments work with financial data.

The form of PPP that will be assessed is the form in which governments will have increased access to user data. This means that the gatekeeper role will be shifted towards governments. This also means that compliance needs for banks decrease, therefore potentially reducing *over-compliance*.

Findings from the framework

The privacy assessment of PPPs reveals a pattern where privacy harms increase substantially while the effectiveness benefits remain questionable. The shift of gatekeeper responsibilities from banks to government creates a fundamental change in the nature of financial surveillance since it moves from commercial compliance to state monitoring of financial behaviour.

Layer	Manifestation in data sharing	Effect on privacy	Comment
Core	*Surveillance* increases as one instance has an overview of transaction data of multiple banks	High	Can increase FEC detection but if non-FEC related data is analysed there is a big privacy risk
Core	*Identification* can increase when data is not pseudonymized properly	High	This is a data-protection issue
Core	*Aggregation* expands, as account data is assembled across banks	High	The goal of data sharing is to reveal complex patterns, this requires thorough analysis.
Enhancing	*Exclusion* increases when users lose transparency about where their data ends up.	Moderate	Transparency decreases as central analysis becomes more opaque
Enhancing	*Secondary use (for AML/CFT purposes)* emerges as data collected for AML could be repurposed for other objectives.	Mixed	Once the data is organized for use within AML use outside AML is possible.
No benefit	*Distortion* decreases as models get more accurate	Beneficial	The impact of false positives grows as detection becomes less explainable at scale.
No benefit	*Insecurity* increases due to concentration of sensitive data.	High	The centralization of pseudonymized datasets raises stakes for breaches. Strong access controls are essential
No benefit	*Increased accessibility* emerges when central units or third parties can access large datasets	Moderate	This risk increases with data sharing as more persons have access to the data. The exact impact is dependent on the amount of automation in this process

Table 6.3: The influence of data sharing between banks on privacy Impact.

Layer	**Manifestation in PPP**	**Effect on privacy**	**Comment**
Core	*Surveillance* expands as banks and state actors coordinate efforts	High	Joint initiatives lead to more visibility of transactions across institutions, which increases surveillance power
Core	*Identification* can increase when governments are given acces to raw data. With pseudonimization this impact might be lower	Mixed	Can lead to more personal data being processed based on state suspicion
Enhancing	*Exclusion* may rise if PPPs reinforce strict profiles without recourse	Moderate	Private actors act on public cues with little transparency; users flagged in PPP models may face denial of services without full explanation
Enhancing	*Secondary use* risk increases when AML data serves other public interests	Mixed	Although PPPs are AML-focused, increased state access creates a risk of data being used for tax enforcement or social security
No benefit	*Insecurity* grows with PPP systems	Moderate	Centralization of sensitive information across sectors heightens cybersecurity stakes; impact depends on data protection protocols
No benefit	*Increased accessibility* of financial data across sectors	High	Broader institutional access

Table 6.4: The influence of Public Private Partnerships on privacy impact.

In this specific type of PPP *surveillance* increases without known improvements in detection accuracy. The framework shows that PPPs increase privacy impacts across multiple dimensions while offering uncertain benefits on money laundering detection.

From a proportionality perspective, PPPs present the most challenging privacy-safety trade-off among the developments assessed. While they may reduce the banks' compliance burden, they do so by transferring privacy risks to a governmental context which only brings more privacy risks.

6.3. Conclusion

To answer the subquestion:

> ”How do key developments in AML/CFT such as AI, data sharing and public-private partnerships, influence the privacy impact of AML/CFT operations?

this chapter applied the privacy framework to three key developments: Artificial Intelligence, data sharing between banks, and public-private partnerships. The framework application reveals distinct patterns in how these developments influence privacy the privacy impact of transaction monitoring. These impacts are summarized in table 6.5

	AI for administration	AI for money laundering patterns	Data sharing	PPPs
Surveillance	Low	High	High	High
Aggregation	Low	High	High	Mixed
Identification	Beneficial	Mixed	High	
Interrogation	Beneficial	Beneficial	Beneficial	
Exclusion	Moderate		Moderate	Moderate
Secondary use in AML	Moderate	High	Mixed	Mixed
Breach of confidentiality			Moderate	Moderate
Distortion	Beneficial	High	Beneficial	
Decisional interference				High
Exposure				High
Increased Accessibility	Beneficial	Beneficial	Moderate	High
Insecurity		High	High	Moderate
Blackmail	Beneficial	Beneficial		
Secondary use outside AML				Mixed

Table 6.5: Assessment of privacy-related effects across different AML/CFT data-processing scenarios.

Artificial Intelligence demonstrates that complexity influences privacy impact.
Section 6.2.1 identified two AI applications with different privacy implications. Automating routine compliance tasks mildly influences*surveillance* impact due to limited training data required, with minimal increase in *aggregation* due to model simplicity. In contrast, using AI to identify complex money laundering patterns requires extensive datasets with civilian transaction data, creating substantial increases across multiple privacy dimensions. The general rule emerging from this analysis is that both privacy impact and AML/CFT benefits are influenced by model complexity

data sharing between banks' privacy impact is dependent on proper pseudonymization and data protection

The framework analysis shows that while pseudonymized data sharing can potentially improve detection of multi-bank laundering patterns, it significantly amplifies the impact of false positives and increases *surveillance* across institutions. The AMLR's restriction limiting data sharing to high-risk customers creates a fundamental tension: limiting further research to suspicious people demonstrates proportionality but it undermines the technology's core purpose of identifying previously undetected suspicious patterns. The TMNL case exemplifies how this regulatory approach can lead to initiative failure without adequately protecting privacy.

Public-private partnerships demonstrate how institutional changes amplify existing problems.
The framework application reveals that shifting gatekeeper functions to public authorities primarily ex-

pands *surveillance* and *accessibility* without addressing the over-compliance friction point. PPPs risk creating mass government surveillance capabilities while perpetuating the same detection inefficiencies that characterize current systems. The combination of state access to comprehensive financial data with the ability to trigger private investigations represents the most significant privacy expansion among the developments analysed.

These developments can combine to create compounding effects. Multi-bank cooperation structures enhanced with AI and coordinated by public organizations would increase both effectiveness and privacy impact exponentially. As the analysis demonstrates, systematic implementation of these technologies together amplifies risks of mass surveillance while the effectiveness benefits remain uncertain.

The answer to research question 3 is that AML/CFT developments influence privacy impact through their interaction with system complexity and institutional structures. Developments that address simple, well-defined problems with limited data requirements can reduce privacy harms, while those requiring extensive data aggregation or institutional expansion create disproportionate privacy costs. The key finding is that while complete protection of both privacy and safety is impossible, unnecessary privacy violations can be avoided through careful consideration of proportionality.

7 Policy advice for proportional AML/CFT

This research is not a philosophy, law or computer science research but it combines these disciplines to create a policy advice that considers al these things together. The contributions of this research will therefore not be in a specific modelling technique, specific law advice or philosophical theory. It will not tell to increase the parameter of model X with 10% and apply methods Y and Z to data storage to solve all the privacy issues there are in the AML/CFT field. The concept of privacy is far too complicated and dynamic for that. Privacy is not about exactly calculating which small scale risks are acceptable but about continuous reconsideration of the large scale implications of these risks. Still, the research has the goal of answering sub-question:

> Which design principles or governance strategies can help ensure proportionate AML/CFT practices in the Dutch banking sector?

Due to the complexity of privacy, this question cannot be answered with a single policy recommendation. Instead, this chapter presents three distinct policy approaches, each grounded in different value priorities. Figure7.1 displays the situation that policy makers are in right now. From the middle point of the diagram, policy makers ideally want to gain privacy and safety. While technology and regulatory changes can realize a move towards this direction, at some point, due to the inherent privacy impact of AML/CFT operations a decision has to be made between privacy and safety. What this decision eventually will be is value based and out-of scope for this research, but when this decision is made, policy makers can be guided towards proportionality. In order to do this, this research suggests three possible policy levers.

1. **Increases in privacy and safety**
   While privacy and safety will ultimately clash and they cannot be respected completely at the same time, the AML/CFT system is not at maximum efficiency yet. There are some structural fallacies in the way the AML/CFT is designed that when fixed could lead to an increase of both privacy and safety. These steps cannot be implemented overnight as they are the result of a very complex system. However, due to their benefit for both privacy and safety, developments in these directions are worth investigating. The fact that these developments seem reasonable from the perspective of this research, does not mean that they are indisputably a good development. Factors such as trusts in banks and governments, development of money laundering techniques, cross border AML/CFT operations are left out of scope for this research. Before implementing the advices from this section, careful analysis of these concepts is recommended. Also it should be considered that while these steps guide society towards the right direction, there is a limit to what they can achieve. At some point a choice has to be made towards either privacy or safety.
2. **Proportional privacy sacrifices**
   When privacy is considered less important then FEC detection and privacy sacrifices become justified for the sake of a safer society, policy makers should still aim for proportionality this means

that privacy sacrifices that do not contribute to a safer society are still not desirable. Using this as a base, some policy recommendations can be made where privacy is damaged in a way that brings proportional safety benefits to society.

3. **Proportional safety sacrifices** When policy makers decide that privacy is too important and that societal benefits of FEC detection do not weigh up against privacy sacrifices, they can move away from FEC detection and towards privacy. This perspective does no longer see privacy as an obstacle but as something that should be protected, even at the cost of detection of FEC.

7.1. Fixes for both privacy and safety

1. **Make the transaction monitoring process more about crime detection and less about compliance**
   There is a tremendous workforce available for the KYC process, that has access to a lot of information. However this manpower and data is used mostly to prevent fines for non-compliance. From the perspective of a bank this is a completely sensible move due to the high fines it might receive for non-compliance. However, looking from a societal perspective this is a waste of resources and disproportionate to the negative impact it has on privacy. A revision of the compliance requirements where the compliance requirements are measured against crime detection could decrease the impact of AML/CFT on privacy while enhancing the greater goal of AML/CFT compliance. There are also things that banks can do to increase efficiency, like using Artificial Intelligence (AI), as shown in section 6.2.1. From a privacy perspective, automating simple tasks can often be an advantage to privacy, even if this initially requires more data.
2. **Minimize the amount of data available to bank employees**
   The interviews led to the insight that bank employees have access to a portal that contains detailed information from all the users of that bank. This is a direct risk according to the harm of surveillance, aggregation and breach of confidentiality as defined by D. Solove, 2006. The personal information of unsuspicious individuals should be protected far more carefully than it is being protected right now. This can for example be done through encrypted vaults that can only be accessed once a transaction from this specific account is marked as suspicious. Not only should this data be made available only when an individual is suspicious, it should also be encrypted again once this bank account is marked as unsuspicious again.
3. **A decrease in false positives justifies the use of opaque models**
   The false positive rate at the moment is over 90% (Ketenci et al., 2021). In other words, 90% of the transactions that are being flagged by models are checked without effect on AML/CFT detection and therefore without a contribution to safety. This number is extremely high and if it can be decreased by using a less explainable model. This is a consideration that can be made. An exact assessment of where this balance lies is dependent on the type of model that is being used and it’s effectiveness

7.2. Value based decisions on key developments

While the developments from the previous section are a step in the right direction, at some point, due to the inherent privacy impact of AML/CFT a choice has to be made between privacy and FEC detection. There are also some pressure points in privacy that have to be adjusted to the governments ambitions regarding the effectiveness of AML/CFT. These pressure points have in common that an increase in AML/CFT effectiveness always comes with a privacy risk. This is all based on the ’processing for a legal obligation’ aspect of the GDPR as described in chapter 4.

Money laundering possibilities are a key incentive for organized crime and making money laundering impossible will most likely eradicate crime with a financial motive. However, the privacy risks that are taken right now rarely weigh up to the benefits of overly thorough data analysis. On top of that, money laundering techniques are evolving just as rapid as the models that detect them which makes it unlikely that the Dutch- or any government will be able to fully prevent money laundering.

This means that policy makers should carefully determine their ambitions regarding AML/CFT effectiveness and the privacy impact this involves. This decision will be made based on values and values change over time. Therefore an iterative approach in which the balance in values is constantly revised and adjusted is recommended. To make sure that policy best reflects the chosen values, a few things can be stated about the developments assessed in chapter 6:

1. **Artificial Intelligence(AI)**
   Section 6.2.1 identified two ways in which AI can be deployed: Automating routine compliance tasks and analysing aggregated transaction datasets to reveal complex laundering patterns. The general rule that emerges from applying the framework is that for low-risk and repetitive chores, AI can replace manual review. This reduces human access to personal data and lowers *surveillance* related harms. On top of that due to the simplicity of the models, the increase of *aggregation* is minimal.
   The second use of AI is identifying complex money laundering patterns. The potential benefits of this are huge, but the privacy harms are as well. Training an AI model with this amount of complexity requires a large and complete dataset. This would mean that the data of a lot of civilians has to be used.
2. **data sharing between banks**
   Isolated transaction monitoring limits a banks view of its own customer base. This makes it hard to detect money laundering patterns that use multiple banks. When banks share pseudonymized transaction details, they can potentially detect complex money flows that would not emerge from single institution transaction monitoring. Despite pseudonymization efforts, data sharing brings big privacy risks. The impact of a false positive would increase since behavioural privacy of an individual is damaged more. The AMLR attempts to mitigate this risk by only allowing data sharing between banks for high-risk customers. While this preserves privacy, it undermines the goal of revealing money laundering patterns individuals that seem unsuspicious when looking from a single bank perspective.
3. **Public Private Partnerships (PPP)**
   When a public authority receives or coordinates transaction data from banks, the gatekeeper function shifts partially into the public sector. In theory, this can reduce over compliance from banks and improve detection by getting the forensic experts closer to the data. The downside of this, is that state access to all user data combined with the ability to trigger private investigation comes with an immense increase in surveillance. Some insecurity risks emerge as well as all financial data will be gathered together. Mitigating the insecurity can be done through good pseudonymization, this means that personal data is only revealed when an extremely high level of risk is reached.

These identified trends can also emerge together. Cooperation structures where multiple banks work together with public organizations are possible. This can even be enhanced with AI. As effectiveness would increase, so would the privacy harms. The risks that come with systematic implementation of AI increase when this is done on more data and when public organizations have access to more data, the risks of mass government surveillance increase. The takeaway here is that while there is no way that both privacy and safety can be protected completely at the same time, there are measures that can be taken to avoid unnecessary privacy violations.

7.3. Real world scenarios based on value decisions

How the previously described considerations actually affect decision making is based on values. These values are hard to pin down for a complete society and even when they are pinned, values can change constantly. This creates the risk of the statements from this research being considered as to complicated or not applicable to society. To demonstrate how these considerations can be applied a policy advise will be written based on three assumed points of view on privacy and safety:

1. Privacy is more important then FEC detection, the AML/CFT system is barely effective as it stands right now and therefore developments in this field for the sake of privacy should be treated with great caution.
2. FEC should be combatted, privacy sacrifices can made for the sake of a safer society.

The real outcome would probably be somewhere in between these three standpoints. Every point is valued equally and depending on cultural and individual every selection on a standpoint can be justified.

The goal of this section is to sketch the practical implications of the framework, not to pass a value judgement and translate this to a policy advise.

7.3.1. Privacy overrules FEC detection

Countries that have low trust in governments, experience with government surveillance, high corruption and low trust in the ability of governments to solve criminal issues. High criminality rate does not necessarily translate to a high willingness to share data. The mere infectivity of AML/CFT operations, that is illustrated by the 0.1% capture rate (Pol, 2020) can also be seen as a reason to value privacy over FEC detection. This means that even if privacy and safety are considered of comparable value, privacy can be seen as more important than FEC detection

If privacy is valued over FEC detection the chances that implementation of the high impact technologies such as AI for money laundering patterns, cross-institutional data sharing or PPPs with direct government access to financial data, will likely not be advised. Implementation of AI for simple administrative can be implemented due to its low privacy impact but this is not a key issue.

On top of the halt on potential innovation, a scale down of the AML/CFT system can even be possible. where mandatory reporting is shrunk and tick-box rules are removed as suggested by Pol 2020 can be recommended, this would contribute to reducing over-compliance as discussed in section 6.1.1, not through innovation but by reducing the need for compliance.

Judge and Kasyap (2024) has formed a concrete list with recommendation for the AML/CFT system. Concrete points they suggest include:

1. **Increase the transaction amount report trigger**
   This was installed at $10.000 in 1970 but due to inflation this transaction amount is far more common now than it was 55 years ago. Increasing this amount would mean that fewer transactions are marked as suspicious.
2. **Detect based on suspicion**
   This would mean decreasing the analysis of transactions of unsuspicious individuals. This is consistent with the AMLR's perspective on data sharing between banks as described in chapter 4 where only data of high-risk clients is shared.
3. **Decrease retention period**
   If data is stored for a shorter period privacy risks decrease

These implementations do preserve privacy but would be a major disruption of FEC activities.

7.3.2. FEC detection overrules privacy

FEC detection can also be valued high, in these cases privacy is seen as a obstacle towards innovation and something that should be sacrificed for the sake of a safer society. This can be the case when trust in governments is high, crime rates are high and there is a societal believe that this can be reduced through AML/CFT operations.

When a decision will be made that privacy is not as big of an obstacle for FEC detection any more, unnecessary privacy risks are still not taken. However, from a proportionality perspective more actions might be justifiable.

1. **Artificial Intelligence for administrative tasks**
   Despite a decrease in the importance of privacy considerations, caution is still required for this implementation. The caution would however shift to a more operational risk perspective. Inaccuracies of automation would eventually lead to more administrative hassle for bank employees which is time consuming and expensive and therefore undesirable.
2. **Artificial Intelligence for complex FEC pattern recognition**
   This promising technique comes with privacy concerns (Oztas et al., 2024), therefore reducing the importance of privacy will speed up implementation. However, developers still have to consider issues with AI that are not related to privacy such as: bias, discrimination and opacity. When this is taken into consideration AI, can be a major contributor to FEC detection.

3. **Data sharing between banks**
   As discussed in chapter 4 the AMLR makes it impossible for banks to discover new FEC behaviour due to privacy issues. Removing privacy as a factor creates room for data sharing structures. From a practical perspective there are more risks than just privacy, when the 5 biggest banks decide to share data and exclude smaller banks from this cooperation the big banks have major benefits in potential cost reductions that the smaller banks do not have, for this some form of government intervention might be necessary.
4. **Public Private Partnerships (PPPs)** PPPs can occur in several forms, the requirements discussed in chapter 6 direct sharing with government reduces over-compliance issues but does not necessarily raise FEC detection rates. When the importance of privacy is reduced, these types are possible but strong governance is required.

7.4. A balanced approach

The previous two approaches sketch what the world would look like with AML/CFT policies that lack nuance, the real world will likely take a bit of both strategies. After all, privacy and financial crime control are not a zero-sum game: both are public-interest goals that serve a different purpose in society. An underestimation of these values would have great societal damage but over-estimating the importance of one of the two aspects would lead to a reduction in the other. A balanced approach would value both values equally and focus on proportionality, this is where the framework from chapter 5 can be of great use. The framework gives insights in the benefits of an action that is impactful to privacy, depending on the needs of society this can help decide whether AML/CFT operation should be increased or scaled down. This means that while concrete measurements such as applying AI or decreasing retention periods can be a great tool for changing the representation of societal values, proportionate policy will always be dependent dynamic, iterative policy measures and continuous awareness of the state of both privacy and safety in society. Combining this with the ability to act at the right time will lead to the eventual answer to the sub-question:

> Which design principles or governance strategies can help ensure proportionate AML/CFT practices in the Dutch banking sector?

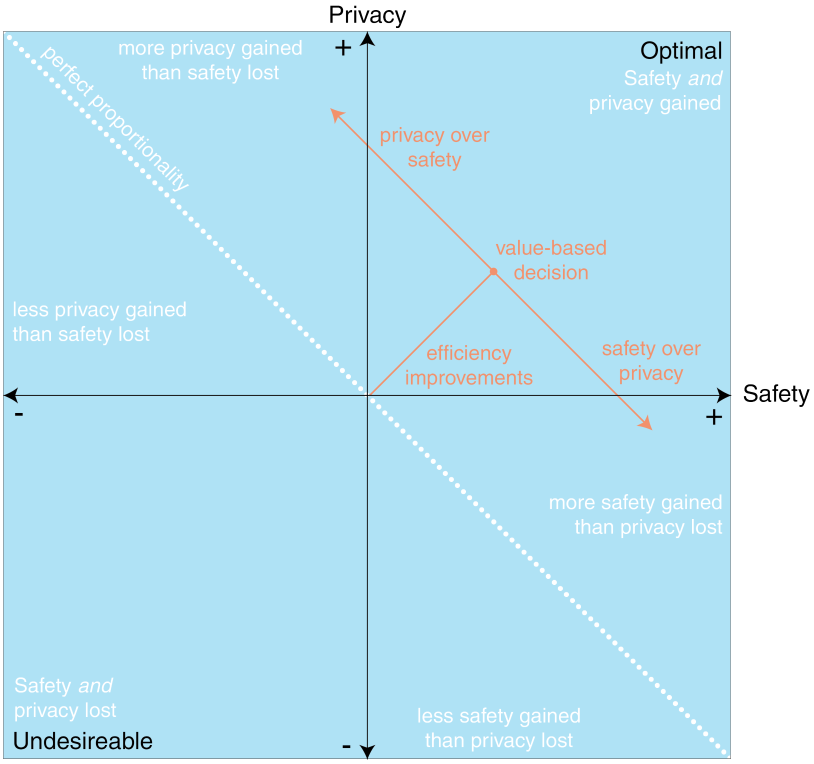

Figure 7.1: Privacy policy measures for a balanced approach

8

Conclusion

The central question of this research was:

> *How can privacy impact be systematically assessed and proportionately balanced against effectiveness in AML/CFT within the Dutch banking sector?*

This thesis finds that privacy impact in AML/CFT can indeed be assessed systematically by isolating three core privacy harms: *identification*, *aggregation* and *surveillance*, and evaluating them within a proportionality framework that weighs these harms against the societal benefits of crime prevention. The study does not claim a universal balance between privacy and effectiveness; the trade-off is value-laden and context-dependent. Proportionate AML/CFT policy therefore requires a dynamic, iterative approach that can reflect changing societal preferences.

A first key insight is that transaction monitoring inevitably clashes with core privacy principles. Because monitoring also brings clear societal benefits, policymakers must decide how they value privacy relative to safety. Both sides of this equation are nuanced. For instance, whether AML effectiveness is judged on the basis of intercepted funds (about 0.1 %) or deterrence depends on data that are difficult to obtain and often delayed.

The framework highlights the privacy aspects of transaction monitoring as follows:

- **Identification** — linking transactions to natural persons;
- **Aggregation** — combining data points to reveal behavioural patterns;
- **Surveillance** — continuous monitoring of account behaviour.

While the framework supports proportionality assessment, moral justification lies outside the scope of any single study because individuals value privacy and safety differently. At present, privacy and AML laws overrule one another, leaving concepts such as proportionality, lawful basis and data minimisation in constant tension. As long as the debate rests on individually variable values, consistency will remain elusive.

The policy advice that emerges is to build an *iteration cycle* in which the importance of privacy and safety is periodically reviewed. A collectively agreed benchmark for privacy would provide clearer guidance on which data may be used and for what purposes. This benchmark should be revisited regularly: a rise in violent crime may justify easing privacy safeguards, whereas creeping surveillance may call for renewed restrictions.

Thus, privacy and AML/CFT effectiveness are not mutually exclusive but must be balanced with care. There is no single, objective answer to what level of privacy sacrifice is justified; that balance depends on shifting social values and evolving perceptions of risk.

The long-term path to balancing privacy, growth and safety is not to fix a point on the trilemma and build technology around it, but to construct a system that can process feedback and make micro-adjustments as values shift. Balancing values, like balancing a physical object, requires continuous small corrections rather than a one-off solution.

Instead of prescribing a fixed equilibrium, this thesis therefore advocates a governance structure that enables *iterative calibration*. Policymakers should periodically reassess how much privacy society is willing to trade for safety and growth, and adapt AML/CFT systems accordingly through feedback loops, monitoring and context-sensitive judgment.

Ultimately, the goal is not to solve the trilemma once and for all, but to build a resilient system capable of responding as priorities evolve. This research provides the conceptual tools, evaluative lens and policy levers for doing so.

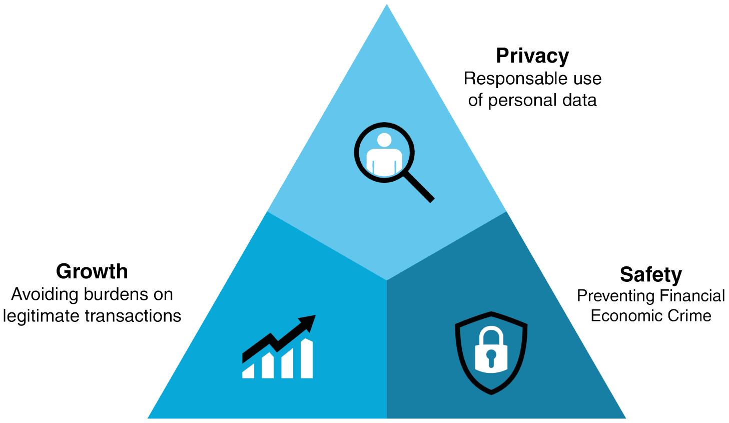

Figure 8.1: The trilemma between privacy, growth and safety

9 Limitations

This research has contributed to guiding the privacy discussion around AML/CFT. It synthesised literature and expert opinions into a framework. The study is exploratory and dives into a complex sociotechnical concept. This makes it far from perfect. This chapter highlights key limitations of the research, their implications and how they influence its applicability.

9.1. Individual values, societal decision

The categorisation of harms is based on factual considerations: it looks at what happens and what this might lead to. However, privacy also depends on cultural and individual values. These cultural value changes can vary even between neighbouring countries. For example, while Germany and the Netherlands are similar in many respects, the share of cash transactions still differs significantly, 22 % in the Netherlands versus 54% in Germany (De Nederlandsche Bank, 2025). This difference is cultural and cannot be linked to a single cause but a clear connection to Germany's recent history[1] has been established (Lichter et al., 2019). Within a country, city or even household, the value placed on privacy can vary, which makes it hard to pin down.

In an AML context, data protection can be seen as a way to safeguard privacy, but it does not guarantee it. Privacy has a philosophical, value-based nature that is difficult to translate into precise rules (D. Solove, 2009). Policy cannot be based on every individual value; somewhere a line has to be drawn to combat FEC effectively. Where that line is drawn will be a political decision. Yet making a choice that dissatisfies many voters is rarely attractive from a political perspective. As a result there will likely still be room for interpretation in the laws, leading to systematic misunderstandings of privacy that can damage safety, privacy, or both.

While the framework successfully identifies these dynamics and can guide policymakers towards their privacy ambitions, it cannot be fully operationalised until those ambitions are explicit. It is therefore essential that policymakers decide how they weigh crime prevention against privacy and communicate this clearly at every layer of society. This decision is not final and will need to be revisited continuously. It is more important *that* a line is drawn than *where* it is drawn.

9.2. Technical specifications of the privacy impacts

This research adopts Solove's (2006) privacy harms as overlapping concepts. "Surveillance" covers every type of monitoring, and any increase in any form is treated as an increase in that harm. In reality, different kinds of surveillance, aggregation and identification each carry their own risks and benefits. An increase in one manifestation of a harm is not the same as an increase in another. Distinguishing

[1] Between 1960 and 1990 the Ministry for State Security (Stasi) conducted one of the most extensive surveillance operations in modern history. At its peak it had one informant for every 6.5 citizens.

these manifestations could make the analysis stronger.

9.3. The connection between money laundering and safety

This study focuses on privacy in the money-laundering debate and argues for privacy-safety proportional policy. By zooming in on privacy, it has not examined safety as a value in equal depth. A crucial addition would be a deeper assessment of how much AML/CFT actually contributes to society. Gerbrands et al. (2022) reviews the effects of AML policy on criminal cash flows but does not explore the link between those cash flows and safety. Nor is it clear how people value safety: do they consider safety for their neighbourhood, country or the world? And because money laundering and terrorism financing are global, how does this translate to local safety and its value?

Answering questions about the influence of AML/CFT on safety would require data that is hard to obtain. It would mean asking criminals to describe how dependent their operations are on laundered money, an unlikely respondent group.

9.4. Societal damage of FEC that goes beyond safety

During this research, FEC has mainly been treated as a threat to safety. While FEC does finance crime and terrorism, it harms society in other ways. It can:

1. undermine good governance and spark political instability (International Monetary Fund, 2025);
2. disrupt economies and undermine market stability (Claver et al., 2023);
3. create an unfair competitive environment(Claver et al., 2023).

Because the study focused on safety, it underestimates these broader societal benefits of detecting FEC. A more complete assessment of AML/CFT proportionality would also weigh these factors.

9.5. Limited technical understanding of the three AML developments

This research discusses data sharing, Artificial Intelligence(AI) and Public-Private Partnerships (PPPs) in an AML context, but it does not analyse their technical implementation in depth. A more detailed technical study could refine the conclusions.

9.6. Argumentation as a main mode of inquiry

This thesis was written for the Engineering and Policy Analysis (EPA) master programme at TU Delft. EPA students learn to tackle problems that involve many stakeholders with conflicting interests; typical EPA theses include simulation to generate data for decision-making (“MSc Engineering and Policy Analysis (EPA)”, 2025). AML/CFT is a grand societal challenge with a strong technological component, making it a good starting point. However, as the study progressed, it became clear that technology was not the main bottleneck—philosophy and governance were.

EPA students are trained to zoom out, understand complex systems and steer towards solutions. Simply producing another model that cannot be implemented would miss the real complexity of AML/CFT. Choosing a less conventional, argument-based inquiry therefore reflects the system understanding typical of an EPA approach.

This departure has limits. One is that argumentation yields fewer immediately actionable insights for policymakers. Embracing the full complexity of the philosophical, technological and legal dimensions leads to many caveats and much nuance. Nonetheless, this is consistent with EPA’s focus on deep system insight.

10 Recommendations for further research

This research dived into the concept of privacy in an AML/CFT context and explores several directions for further implementation. Its explorative nature makes it a source of inspiration for a wide variety of follow-up research projects. These projects could not be executed within the available time and resources; therefore a list of suggestions is provided below.

10.1. Combatting over-compliance and revising the gatekeeper position of banks

From both a privacy and a safety perspective, the gatekeeper role of banks is under significant pressure. AML/CFT policy is not only impactful to privacy but also intercepts only a small fraction of criminal cash flows (Pol, 2020) and is financially costly (NOS, 2025).

The findings in this research invite a careful reconsideration of what society should expect from banks. The hunt for money-launderers is often compared to a game of cat and mouse: banks (cats) are in constant pursuit of criminals (mice), who have countless places to hide. From the perspective of the cat, this can feel like a losing battle, as only a portion of the targets are caught. However, the value of a cat is not merely the number of mice it catches, but the fact that mice avoid a house that smells of cats.

Translating this analogy to AML/CFT, the fundamental question for policymakers is whether they adopt the perspective of the cat or of the homeowner. Future research could explore this philosophical point and examine models of deterrence versus detection and the role of perception in effective AML/CFT policy.

10.2. Specifications on the law

Chapter 4 shows that current laws are unsuccessful in defining clear privacy guidelines specific to AML/CFT. This is largely due to the conceptual complexity of privacy. Although this research explored methods for structural proportionality assessment, key concepts such as “proportionality,” “data minimisation” and “legal obligation” remain undefined in the AML context. Follow-up work could focus on:

- **Clarifying purpose limitation**
  Legal interpretations of “purpose limitation” are vague, especially where AML/CFT reuses data. Further study could show how regulators might define clear primary purposes for data collection and enforce boundaries for secondary uses.
- **Creating legal thresholds for suspicion levels**
  AML surveillance operates without a tiered approach to suspicion. Research could establish differ-

entiated surveillance permissions based on defined suspicion levels, mirroring criminal-procedure principles.

- **Specifying the primary purpose of transaction data**
  Future studies could propose statutory definitions of “primary use” and recommend mechanisms to regulate secondary use, including sharing with FIUs and law-enforcement agencies.

A legal scholar could build on this research and translate these methods into laws that capture privacy more effectively.

10.3. Dynamics between privacy impacts

Two interactions between harms deserve closer attention:

- **Harms that strengthen one another.** Knowing a sensitive story about an unknown person and being able to identify that person are relatively harmless in isolation, but combined the impact increases.
- **Harms that can cancel one another out.** In transaction monitoring, once a specific point of information (e.g. “is this customer laundering money?”) is established with confidence, additional data collection may be unnecessary. Hence an increase in one harm can reduce another.

10.3.1. Impacts that can (partially) cancel each other out

Assuming banks are profit-driven and will not expend additional monitoring effort once their legal obligation is met, an increase in one harm might reduce the need for others.

- **More surveillance to reduce interrogation and decisional interference** Greater *surveillance* can spare civilians other harms. With richer data, staff need not request additional information, and more accurate surveillance can lower intrusive decisions about account restrictions.
- **More aggregation to reduce exclusion** If *aggregation* increases, the grounds for suspicion become more explainable, allowing greater transparency. Yet excessive detail could reveal detection logic, aiding money-launderers.

10.4. Privacy-preserving technologies

As stated in Chapter 2, many privacy-preserving technologies aim to reduce the privacy–safety dilemma. The main critique is that without clarity on which aspects of privacy must be preserved, these techniques remain under-exploited. Two suggestions are given below but off course many other techniques can be explored.

- **Differential privacy** adds mathematically calibrated noise to statistics or model updates so that any single customer’s data has only a negligible influence on the output (C. Xu et al., 2023)
- **Federated learning** trains a shared model across multiple servers. Each sub-model is trained locally; only parameter updates are exchanged. One study reports a 20 % reduction in false positives (Suzumura et al., 2022). However, isolated implementation cannot track users across banks. one of the key advantages of cross-institutional sharing.

10.5. Position of financial privacy in the broader privacy discussion

This research focuses on financial privacy within AML/CFT, implicitly treating AML/CFT as the principal privacy threat. Yet privacy is already diminished in many other domains such as: social media, e-commerce, advertising, smartphones. If the societal baseline is already low, reducing AML measures may not greatly improve overall privacy. Future work should place financial privacy within this wider surveillance ecosystem and study how AML/CFT policy interacts with other data-intensive practices.

10.6. Different types of FEC and their societal impact

Proportionality analysis should also weigh the nature of the FEC investigated. There is a clear difference between undeclared earnings used for personal expenses and complex laundering of terrorist funds. Forensic investigation to dismantle a transnational drug cartel may be reasonable; taking the same measures to uncover that someone used € 100 of undeclared income to buy groceries appears less proportionate.

Further research could examine how different FEC types cause different societal harms and how this should influence surveillance intensity. This could lead to more calibrated, efficient and ethical AML systems.

A
Methodology

This research applies several philosophical theories to privacy with the ultimate goal of guiding model builders, bankers and policy makers towards a privacy friendly AML system. This knowledge is gathered using three main data sources: literature, interviews and argumentation. This translates to a combination of the modes of inquiry: *argumentation, conceptualization, observation* and *evidence synthesis*.

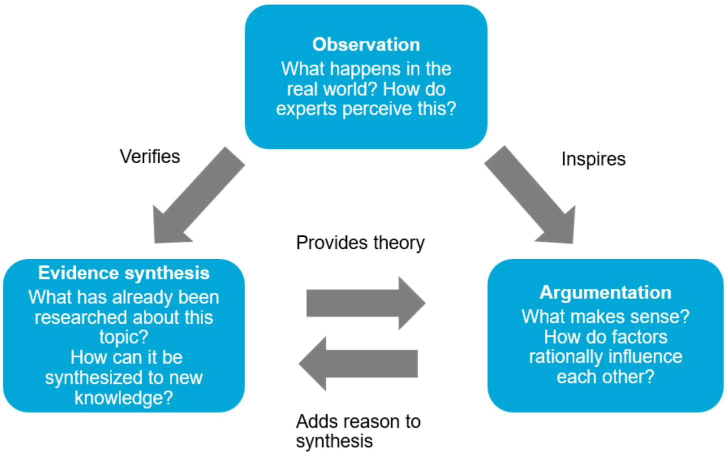
Observation
What happens in the real world? How do experts perceive this?
Verifies
Inspires
Provides theory
Evidence synthesis
What has already been researched about this topic?
How can it be synthesized to new knowledge?
Argumentation
What makes sense?
How do factors rationally influence each other?
Adds reason to synthesis

Figure A.1: The relation of the three modes of inquiry

A.1. Argumentation or conceptualization

The goal of this thesis was finding a right way to protect privacy in transaction monitoring. This has two aspects: a technological side in which the system is designed to protect privacy at every step, and an ethical side in which the ’right way’ is defined. The ethical side of this goal is so wicked that it is not even clear what is right and what is wrong. This means that defining the goal has to be the first step. A lot has been written about privacy but it is rarely seen as a core value for AML/CFT design. This means that in order to do this, new things have to be created out of the already existing research.

The best mode of inquiry was argumentation, structuring the information from research, theories, laws and expert opinions to make a solid argument for which degree of monitoring is the ’right’ way. This mode of inquiry is was what made the research unique and can therefore be seen as the key mode of inquiry for this research.

This is very non-typical for an Engineering and Policy Analysis (EPA) thesis as EPA is all about quantifying problems, making models and creating argumentation based on data- not on thoughts. However, as argued in 2, transaction monitoring is a multi-billion euro industry in the Netherlands already. This creates the assumption that banks are already putting in a lot of manpower, and funding to make the models better. If this is the case, it is very unlikely that the limited resources of this research would be able to improve the technical aspect of these models significantly.

Another thing that distinguishes EPA from other educational programs is a multi-disciplinary angle, this holistic system approach can lead to unique insights that can not be found when only looking at one component of the system. These insights can then form the basis for models that perform better according to a complete understanding of privacy instead of solely focussing on optimizing one variable. This thesis decided to focus on exactly that by looking at a soft value as privacy with the perspective of a systems engineer.

A.2. Observation

The power of using argumentation as a mode of inquiry is that it allows for a more creative workflow, the big downside is that it is hard to verify by itself. Especially if the research is only conducted by one individual. That is why the argumentation is backed up by observations. For this three options are common: Interviews, Case study and surveys (Bhatta et al., 2024)

For this topic, a survey could be conducted to investigate how privacy is perceived. This could give insights in how privacy should weigh against the harms of money laundering which could be the basis for a privacy policy that serves society. However, this is not the most accurate way of gathering this information. When reading chapter 5 it gets clear that the importance of privacy is structurally undervalued. Asking people how much they care about their privacy and what they would be willing to do to protect this would lead to a conclusion that builds up on this structural undervaluation. This means that for the validation of the theories that originate from the argumentation, it is not about how much respondents there are available, but about the expertise of the subjects and the depth of the interviews. That is why expert interviews where conducted.

These interviews used a semi-structured approach and had the intention of finding how data is processed in transaction monitoring, which types of analysis are being conducted and how the future of transaction monitoring will look.

On top of that information was extracted from the emerging trends paper written by KPMG in may 2024. This paper contained 15 elaborate interviews with key actors in the AML/CFT field. They where asked how the future of AML will look. The completeness and the many perspectives made this paper an amazing source. However, while privacy was mentioned in almost every interview, it was rarely the main topic of discussion.

The broad analysis of future trends and the specified expert opinions on privacy allowed for observation of the status quo which allowed for a combination of empirical and rational analysis of the problem.

A.3. Evidence synthesis

Evidence synthesis is a mode of inquiry where empirical interferences are made not based on direct observation, but rather by collecting and evaluating an already existing body of knowledge that answers a research question (Bhatta et al., 2024). In this research a lot of already conducted research is used. This is an essential step in verifying the knowledge acquired by argumentation.

The already conducted research also inspires ideas that come from the argumentation section.

By combining existing academic literature, legal texts, policy documents, and expert insights, this research ensured that the conclusions drawn from argumentation were not just theoretical but grounded in a broader empirical foundation. The synthesis of these sources enriched the argumentation process and provided the necessary validation to position the proposed privacy framework within the real-world context of AML/CFT policy and practice.

B

Statement regarding the use of Artificial Intelligence(AI)

The philosophical nature of this research lead to great caution regarding the use of AI. A big part of a convincing philosophical research is in how findings are put into words. For this research there where some experiments in which large language models where used to produce text but this, rarely lead to satisfactory text. This research was also dependent on creativity to look at the privacy problem from a different angle, the ultimate goal here was to think things that have not been thought yet. Using a language model that is trained on old research felt like a limitation of this creativity. However, AI has played a significant role in the development of this research. It increased efficiency in a lot of key tasks and sometimes even inspired new ideas. Example roles of Artificial Intelligence have been:

- **Language checks**
  AI has proven very useful to point out spelling, or grammar errors. It also was ideal for putting text into the LaTeX format. These tasks saved a lot of time and contributed to a professional appearance of the report.
- **Referencing**
  The prompt that has been used the most for this research is: Generate BibTeX citation for (url). This is a simple administrative task for which AI was perfect.
- **Literature search**
  First of all, some AI tools have been used to scan papers for relevance. After the AI tools identified key aspects of a potentially interesting paper, the papers where read manually. On top of that, AI tools have been used to gather sources about specific details.
- **Restructuring**
  As the research got bigger it was harder to keep track of the organization of the text. AI in identifying which concepts where repeated to much, and which concepts could use some more clarification.
- **Brainstorming**
  In this research there have been moments where it was hard to put a thought into a coherent story. AI tools proved very useful in these moments.

For this the following models have been used:

- **ChatGPT(Open AI)** Was used for the standard tasks like summarizing or translating.
- **Copilot (Microsoft)** Was used similar to Chat GPT
- **Claude(Anthropic)**, Was used sporadic at the beginning since it is known to be better for processing text. While the text was indeed more natural it failed to capture the essence of original ideas s
- **Perplexity** Was used to find scientific sources about a specific topic.

- **NotebookLM(Google)** Was used for the transcription of the interviews.

While AI tools have contributed greatly to this research and the product would never have been what it has been without the availability of AI, it was always used responsibly and without harm to the authenticity and integrity of this research.

C

Key authors and their foundational works

C.1. Daniel J. Solove

Daniel J. Solove is a leading scholar in the field of privacy law and policy. He holds the John Marshall Harlan Research Professorship at Georgetown University Law Center, where he teaches courses on privacy, torts, and administrative law. Over the past two decades, Solove has published extensively in peer-reviewed law journals and through major academic presses. His work is frequently cited by courts, regulators, and fellow academics, in part because he consistently combines rigorous doctrinal analysis with insights drawn from empirical studies and sociological data. Solove's prominence arises not only from the volume of his scholarship but also from his role as a frequent advisor to both governmental bodies (e.g., the U.S. Federal Trade Commission) and private-sector consortia developing privacy best practices. As such, Solove's analyses are widely regarded as both theoretically sophisticated and practically relevant(D. J. Solove, 2025).

C.1.1. A Taxonomy of Privacy (2006)

Published in the *University of Pennsylvania Law Review*, "A Taxonomy of Privacy" extends the questions raised in *Understanding Privacy* by offering a systematic classification of privacy harms. Rather than starting with "What is privacy?" Solove inverts the inquiry: "What can go wrong when privacy is violated?" He then groups potential harms into four broad categories—Information Collection, Information Processing, Information Dissemination, and Invasion—each containing multiple subcategories (e.g., "aggregation," "identification," "intrusion," "exposure"). This taxonomy accomplishes two crucial goals:

1. **Analytic Clarity:** By enumerating specific, recognizable harms, the taxonomy helps legislators, regulators, and compliance officers pinpoint which privacy interests are most at risk.
2. **Policy Guidance:** It provides a common vocabulary to compare otherwise disparate data practices. For example, in AML systems, a bank's decision to log every micro-transaction can be assessed as "surveillance" (Information Collection) and "aggregation" (Information Processing).

Because this article has since become a touchstone among privacy scholars, its categories regularly appear in regulatory impact assessments (risk-based AML frameworks) and academic treatments that explore how to balance privacy against other values. Within this thesis, Solove's taxonomy is directly invoked in Chapter 6 to classify and evaluate which types of privacy are inherent in transaction monitoring.

C.1.2. Understanding Privacy (2008)

In *Understanding Privacy*, Solove vouches against the search for a single, universal definition of "privacy" and instead examines how various activities and social practices threaten individual autonomy, dignity, and personal identity. Drawing on case law, behavioural science, and sociological reports, he identifies five "groups of concerns" that underlie most privacy debates:

- **Information Collection** (surveillance, interrogation)
- **Information Processing** (Identification)
- **Information Dissemination** (breach of confidentiality, exposure)
- **Invasion** (intrusions into physical space, decision interference)
- **Lack of Transparency and Consent**

By moving away from a single concept of privacy, Solove shows why debates over new technologies cannot be resolved by a single rule (e.g., "all data gathering is bad"). Instead, policymakers and practitioners must ask: What specific harms does this practice threaten, and how do those harms interact with other social values? In the context of AML/CFT, *Understanding Privacy* supplies a meta-framework for identifying which dimensions of privacy (e.g., aggregation versus surveillance) are implicated by different transaction-monitoring measures.

C.1.3. On privacy and technology (2025)

While the two previous works of Solove are great for creating a basic understanding of privacy, they are slightly outdated. As technology advances, both computing power and information collection increase. This means that the role of privacy is changing as well. This work talks about these developments in privacy. The key themes are as follows:

- **Rethinking privacy in the digital era**
  Solove challenges common metaphors and misconceptions like: assuming AI is 'intelligent' or believing regulation necessarily stifles innovation. Instead, he insists privacy must be viewed deeply and socially, not as mere individual preference
- **Technology-driven transformations**
  Solove unpacks how innovations(especially Artificial Intelligence(AI)), affect privacy through data collection, profiling, automated decision making, interference and prediction.
- **Power imbalances & legal gaps**
  Solove contends that power drives privacy violations and that current laws are inadequate. He debunks the myth that companies will self-regulate, or that users alone can defend their purposes.
- **A path towards accountability**
  The book suggests a 'bolder path' for law, this is rooted in ethical judgement, accountability and systemic change. Solove argues that individuals should not be left to fend for themselves. Instead legal frameworks should hold corporations and governments responsible.

The book was published in march 2025, which was in the middle of the process of writing this master dissertation. It has formed a major source of inspiration for many findings in this research, it also takes into concerns of Soloves older works and revises them. In this research Solove talks about older works like 'A taxonomy of privacy' and reflects on the applicability in todays age. Here he states that while the taxonomy is old, after revision he would not change anything fundamental (D. Solove, 2025)

B.2 Roger Clarke

Author Background and Reliability Roger Clarke (1948–2021) was an Australian computer scientist and policy researcher best known for his early and sustained critique of data surveillance practices. During his tenure at the Australian National University and later at the University of Technology Sydney, Clarke pioneered the study of how information technologies enable new forms of "dataveillance." He advised governmental committees on privacy and e-government initiatives, and his writings are routinely cited in international privacy guidelines (e.g., OECD, European Commission). Clarke's reputation rests on decades of interdisciplinary work bridging computer science, law, and public policy. His analyses combine technical accuracy (he was fluent in system-architecture design) with policy sensitivity, making his essays lasting references for both academics and policymakers.

B.2.1 “What Is Privacy?” (1996)

In the article “What Is Privacy?” (originally circulated as an electronic bulletin paper in 1996 and subsequently widely reprinted), Clarke defines privacy as the “claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” Crucially, Clarke distinguishes between:

1. **Information Privacy** (control over personal data)
2. **Bodily Privacy** (protection of physical selves from invasive procedures)
3. **Privacy of Communications** (confidentiality of correspondence)
4. **Territorial Privacy** (control over physical or virtual spaces)

His principal contribution in “What Is Privacy?” lies in three observations:

- **Process-Oriented Definition:** By focusing on individuals’ control over flows of information (as opposed to preserving a static “zone” of privacy), Clarke captures how modern computing systems continuously mediate data.
- **Hierarchy of Contexts:** Clarke argues that privacy cannot be understood outside social and cultural contexts; what counts as a “private” matter varies across societies and technological eras.
- **Dataveillance Emphasis:** He introduces the term “dataveillance” to describe the systematic use of computers to monitor and store personal data. Unlike traditional surveillance (which often requires a physical actor), dataveillance occurs passively, in the background of routine transactions.

Within this thesis, Clarke’s definition undergirds the conceptual separation between “identification” and “aggregation.” For example, when a bank retains digital logs of every debit-card swipe, it engages in dataveillance—even if no human examiner ever reviews the record. Clarke’s insistence that privacy is fundamentally about “claiming control” over data flows makes it clear why individuals subject to AML checks may feel their autonomy undermined, even if all procedures comply with statutory requirements.

B.3 Importance of These Authors’ Works

The works of Solove and Clarke have inspired this research further than the many citations it uses. Their nuanced understanding of the complexity of privacy has been so influential that it altered the way the Author thinks about the concept of privacy. While the findings of these authors where never taken as absolute truths, their findings sparked a vision on privacy that echos through this entire research.

D

Expert validation

To test whether the privacy-effectiveness balance propsed in chapters 5 and 6 the framework was matached with three sources: KPMG's trend studies, sector-wide proposition papers and semi-structured interviews with AML/CFT experts. There are variations in the details of these sources but they are consistent in vouching for smarter and better-target monitoring. Privacy ambiguities and practical obstacles are also identified as the main drag on innovation. A more detailed documentation of the expert validation can be found in appendix E

D.1. Emerging trends - KPMG

In 2024 KPMG the Netherlands published: *Emerging Trends: Navigating the Future of the FEC Compliance Landscape* This paper provides a thorough analysis of the evolving AML landscape, particularly within the Netherlands. Based on interviews with financial institutions, regulators and industry experts, the report identifies several key trends shaping the future of AML compliance. The expert opinions of this research has been at the base of the developments that where assessed in chapter 6.

D.2. Insights from KPMG's Emerging Trends study

The 2024 KPMG report, based on fifteen industry interviews, identifies three forces reshaping Dutch AML: risk-based profiling, cross-bank data sharing and AI-enabled pattern recognition (KPMG Advisory N.V., 2024). Supervisors at *De Nederlandsche Bank* (DNB) confirm the direction of travel: they want banks to "move away from box-ticking" and let profiling intensity rise only as customer risk increases. *Rabobank* echoes this ambition but urges regulators to "pull"specific intelligence instead of demanding ever broader data dumps; fewer analysts with deeper expertise should replace mass alert handling.

Both the *FIU-Netherlands* and the *TMNL* consortium go a step further. They regard joint analytics as indispensable, yet warn that pseudonymisation is *not* anonymisation and that the present system "would look entirely different if redesigned from scratch". Interviewees from KPMG's own forensic practice argue that large-scale machine learning can already protect privacy by surfacing only the riskiest cases for human review. A professor of financial law counters that such efficiencies matter little unless the state invests more in its own investigative capacity and trims today's bloated KYC workforce.

Banks themselves converge on two themes. *ABN Amro* and *Vartion* anticipate a decade of expanding public-private partnerships (PPP) and greater reliance on explainable AI, but insist that algorithms remain reproducible and auditable. Market-watchdog *AFM* and sustainable bank *Triodos* caution that data-driven supervision must not lapse into tick-box compliance or unchecked profiling of ordinary customers.

D.3. Combined forces - KPMG

In 2023 KPMG the Netherlands wrote a report on the possibilities of Public Private Partnerships(PPPs) and which concerns they bring. The report also covers different types of PPPs these PPPs and their privacy impacts are displayed in table D.1.

PPP type	Description	Privacy concerns	Remarks
Public-Private Data Sharing	Collaboration between government agencies and private entities to share data for AML/CFT purposes.	Risks include potential misuse of data, lack of transparency and challenges in ensuring data accuracy.	Needs strong legal basis and oversight to ensure accountability.
Joint Monitoring Initiatives	Collaborative efforts to monitor transactions and identify suspicious activities.	Potential issues include over-surveillance and the need for robust data governance frameworks.	Can lead to profiling without due process; safeguards needed.
Centralized Databases	Creation of shared databases for storing and analyzing financial data.	Challenges include securing the data against breaches and ensuring access controls are in place.	High-stakes data aggregation increases systemic privacy risk.
Federated Learning Models	Decentralized approach where data remains within the organization and only insights are shared.	While more privacy-preserving, it requires sophisticated technology and coordination.	Promising solution if implemented with transparency and verification.

Table D.1: Types of Public-Private Partnerships (PPPs) and associated privacy concerns

D.4. Nextgen gatekeepers - Nederlandse Vereniging van Banken (NVB)

In 2024 the NVB produced a report in which they revised the gatekeeper role of banks. The report aims to make AML/CFT efforts more effective and proportionate, reducing unnecessary burdens on well-intentioned customers while enhancing the detection of suspicious transactions. The reports four key pillars are:

1. **Jointly set priorities under national coordination**

   Both public and private resources are scarce. The paper therefore calls for a *National Coordinator Anti-Money-Laundering* who convenes public and private actors each year to agree on the most urgent ML/TF threats. A shared agenda ensures that manpower and data are channelled toward the highest-impact risks, improving the relevance of bank reports and the strike rate of law-enforcement agencies.

2. **Forensic intelligence as the starting point**

   The NVB urges a shift from today's *push model* in which banks mass file "unusual" transactions to a *pull model* in which police, FIU and tax authorities supply targeted intelligence that triggers focused data requests. Experience from terrorism-financing and serious-crime taskforces shows that such intelligence-led requests produce a much higher proportion of FIU "hits" than screening.

3. **Continuous vigilance for new trends and patterns**

   Criminal typologies evolve rapidly. Banks therefore need to run permanent cross-institutional trend and pattern analyses, building on concepts pioneered by Transaction Monitoring Netherlands (TMNL). The paper links this "trend alertness" to an ongoing dialogue with public authorities so that emerging threats feed straight back into the joint priority list.

4. **Phasing out low-value measures**

Broad, undifferentiated KYC and transaction monitoring now yield an estimated 95 % false-positive rate, burdening legitimate customers and eroding public support. Once better risk intelligence is in place, banks, together with the central bank (DNB) and privacy regulator (AP), should scale down controls that add little value. The position paper proposes an *evidence framework* that lets banks show which controls can be retired without weakening AML/CFT outcomes.

E

Interview strategy

This appendix contains two parts:

1. **Interview question sets** (the guides used during each semi-structured interview);
2. **Raw interview notes** per respondent (verbatim bullet-point summaries).[1]

E.1. Interview question sets

E.1.1. General questions on transaction monitoring

- Can you describe the key steps involved in the transaction monitoring process from the creation of a transaction to a potential FIU Report?
- When analysing transactions, is there a distinction between business related data, and private data?
- How long is data stored? How is it organized?
- Are minors being monitored the same as adults?
- When a transaction is flagged as unusual, which data is being made insightful for the KYC analyst? About this specific transaction but also all transactions made by this same data subject?
- Can a KYC analyst also see transactions from people who are not under surveillance?
- What is the risk assessment that is done for business accounts generally based on?
- Is there feedback from a FIU on whether a suspicious transaction is really illegal?
- Does a KYC analyst monitor every transaction individually or is he looking at patterns?

E.1.2. Questions on data sharing and privacy

- How common is the issue of an incomplete picture due to not enough information from other banks?
- are the privacy concerns associated with data sharing in AML processes?
- How can banks ensure compliance with data privacy regulations while sharing information for AML purposes?
- What measures can be taken to protect sensitive customer information during data sharing?
- What are the privacy concerns associated with data sharing in AML processes?
- How can banks ensure compliance with data privacy regulations while sharing information for AML purposes?
- What measures can be taken to protect sensitive customer information during data sharing?

[1] For transparency, no sentences or statements have been removed. Formatting changes serve only to improve readability.

E.1.3. Questions specific to the Dutch TMNL initiative

- Banks shared their data with each other through an independent foundation called TMNL, how was the ownership structure of TMNL?
- How was the data anonymized between banks?
- Did TMNL use behavioural analysis? and if so, which privacy precautions did they take to do this?
- What was the increase in effectiveness during the TMNL initiative
- What technologies and methodologies are used in TMNL to facilitate data sharing and transaction monitoring?
- How does TMNL address privacy concerns while enabling effective data sharing among participating banks?

E.2. Notes from the KPMG Emerging trends paper

E.2.1. I1: DNB

- Moving to a risk-based approach where clients are profiled based on risks. *Consistent with the finding that profiling intensity should increase as clients are put into a higher risk category.*
- Focus has been too much on technical compliance; we should move away from that and focus more on the goal of TM. *This might be a tension field since privacy by design is based on systemic technological requirements.*
- Too many grey zones in AML compliance. *Very consistent with the statement made in chapter 6; when the rules of compliance are not clear, they are harder to follow.*
- A paradigm shift: institutions need to take a more holistic approach towards client management. The goal is to reduce segregation between seeing clients from a CDD perspective and from an ESG perspective. *This is in line with the fiduciary relation between banks and their customers.*

E.2.2. I2: Rabobank

- Banks are effective in their efforts to combat money laundering despite the criticism of it being costly. However, a pull approach is preferred in which specific information is requested from financial institutions. *This is in line with the 'less fishing trips, more whale hunting' statement made in 6.*
- In the future, there will be fewer analysts with a higher level of expertise. *In line with the requirement defined in 6.*
- Transaction monitoring will be more successful if it can be done across different banks, following the approach of TMNL. This needs caution; the benefits of TMNL were not yet clear according to one of the interviewed experts. According to Solove's principle of Aggregation as described in chapter 5 and the theoretical knowledge about re-identification as described in chapter 2.

E.2.3. I3: FIU Netherlands

- The FIU is convinced that becoming more effective in the fight against FEC requires increased public-private and private-private partnerships. TMNL is an example of this. *Here again, caution is needed; pseudonymized does not mean anonymized.*
- The FIU recognizes that obligations imposed on the private sector also require that public sector parties facilitate the private sector in enhancing their preventive frameworks.

E.2.4. I4: TMNL

- The fight against money laundering is going well if you look at the most recent assessment by the Financial Action Task Force (FATF).
- A closer look at the results reveals that they pale in comparison to the efforts that are made.
- If you could redesign the money laundering approach from scratch, it would not look the same. The trick is to say goodbye to the current system.

- TMNL fits in this approach. ”If we see better what is wrong, we also see better what is right.” *Not quite true if you look at the harms as described in 5.*
- We understand that there is a delicate balance between privacy and anti-money laundering that is not a mathematical formula; it is about proportionality.
- The European Anti-Money Laundering Regulation represents a tipping point. The central aim of the regulation is to protect citizens.
- The AMLR claims to have found a balance between the importance of privacy and money laundering. However, privacy is too dynamic to be defined forever.
- What the AMLR does well is leaving room for gatekeepers to collaborate.

E.2.5. I5: KPMG

- (Non-conscious) AI models evaluating a large corpus of data and then providing humans with only a limited set of data is already privacy preserving.

E.2.6. I6: Prof. Financial Law

- Gatekeepers, public parties and politicians play a crucial role.
- There has been increasing criticism against the government for not allocating sufficient resources to combatting money laundering. This is a political choice. The central government should pick up its role in fighting financial economic crime.
- Public-private partnerships are believed to be the solution for this.
- The number of KYC analysts should shrink since costs are too high and effects too low.
- The number of systems used for KYC should be lower. Preferably a standardized approach for similar instances.

E.2.7. I7: ABN Amro

- In the next 10 years there will be an increase in PPP.
- AI can be effective, but only when there is enough data. *This connects to privacy concerns.*
- The mix between systems and analysts will shift toward analysts.
- We do not need more regulation; we need more cooperation. A better understanding of what is “usual”, typologies, and when detection is effective.
- Banks are responsible for AML policy implementation because of their central role.
- Stresses the importance of making the AML system future-proof.
- Outcomes of AI should be reproducible.

E.2.8. I8: Vartion

- Financial crime prevention can benefit from AI in multiple ways, two of which are: using it to automate parts of the flagging process and to automate parts of compliance that financial institutions must execute.

E.2.9. I9: AFM

- AFM is shifting towards more data-driven supervision. Simultaneously, digital crime is also on the rise.
- It is crucial to strike the right balance between privacy and fighting criminal activities.

E.2.10. I10: Triodos

- In recent years, there has been a significant focus on technical compliance, which resulted in financial institutions adopting a tick-the-box approach to compliance.
- There are underground banking conferences where criminals exchange information on monitoring rules used by banks.

- Vouches for a national crime prevention strategy.
- There is no benchmark in what is unusual and what is not.

E.2.11. Interview 1: General banking system

- The data flow of a transaction within banks involves several steps: the transaction passes through bank-specific models (such as sanction models and TM models, which vary by scope), may trigger an alert, and is then assessed, often by an analyst. The setup varies significantly across financial institutions.
- There is a distinction between transaction filtering (TF) and transaction monitoring (TM). Filtering blocks sanctioned transactions, while monitoring detects and reports potentially suspicious transactions.
- Sanctions lists exist at national, EU, OFAC (US), and UN levels and include individuals, entities, goods (such as dual-use items), ships, etc.. Banks choose lists based on their risk appetite. Filtering against sanctions lists is typically automated and blocks the transaction.
- Banks are always responsible for transactions processed through their systems. If a sanctioned transaction is allowed through, the bank is liable, regardless of whether it involves their own customer. Monitoring focuses on whether money laundering could reasonably have been detected.
- The Dutch Central Bank (DNB) supervises banks by examining their governance and the processes they have in place to detect suspicious activities. The focus is on documented procedures and their demonstrable effectiveness, rather than on individual transactions. DNB also assesses the bank's risk appetite, which influences the types of controls implemented.
- A KYC analyst has access to basic customer data, transaction history, and can request additional documentation. They analyse customer patterns and relationships and may ask customers for clarification regarding suspicious transactions.
- There are no clear data-retention policies; data retention periods apply, such as when a customer relationship ends.
- Analysts' access to customer data must be purposeful; browsing out of curiosity is not allowed in principle, although enforcement varies by institution. Access can be logged.
- Customers are periodically reviewed from a risk perspective (risk classification), not only in response to alerts. Higher risk classes lead to more frequent reviews. Risk factors include customer behaviour and the sectors in which they operate.
- De-risking refers to the termination of customer relationships when risk is deemed unacceptably high; this may affect innocent individuals. High risk can also result from lack of cooperation from the customer.
- Banks usually report dossiers (based on behaviour and combined data) to the FIU, rather than individual transactions. The FIU, as an investigative body, can request data from banks.
- Customers do not have full privacy over their transaction data due to the legal obligations of banks. Banks' terms and conditions reflect this.

E.2.12. Interview 2: Key findings on TMNL

- TMNL (Transaction Monitoring Netherlands) was a collaboration between five Dutch banks aiming to identify complex money laundering structures and new patterns that are not visible through monitoring at a single bank.
- The primary reason for terminating TMNL was the anticipation of upcoming European AMLA (Anti-Money Laundering Authority) legislation. AMLA only allows data sharing between banks if there is already an indication of elevated risk, while TMNL aimed to detect risk before it became apparent. The exact implications of AMLA are still unclear.
- Under the GDPR, there was fundamentally no legal basis for banks to share data in the way TMNL intended, unless explicitly allowed by law. A planned amendment to the Wwft to enable this was delayed. AMLA restricts national discretion in this area.
- The initiative received negative public attention, partly following an article by Follow the Money.

- TMNL claimed it was effective, but receiving banks were not always convinced. The initiative operated on a minimal scale and limited datasets. Banks had to pre-filter data before sharing it, which hampered effectiveness. Its value had not yet been fully demonstrated.
- Exact details of the shared data remain uncertain. Data was likely not fully pseudonymized or anonymized to allow linking. Shared data primarily involved transactions with large companies. The focus on companies partly stemmed from an interpretation that privacy laws offer stronger protection for individuals than for businesses.
- TMNL was an external foundation established by the banks.
- TMNL had no direct connection to the FIU; it returned alerts to the banks, which were then responsible for investigating and potentially reporting to the FIU.

Privacy, legal, and ethical challenges (cross-interview themes)

- The fight against money laundering and terrorist financing inherently conflicts with privacy. Detecting complex patterns often requires access to large amounts of data.
- There is tension between the obligations under the Wwft (which mandates monitoring) and GDPR principles, such as data minimization. Although the Wwft provides a legal basis, the scope of data needed for complex analyses remains vague.
- The current interpretation of the Dutch Wwft restricts outsourcing of “ongoing monitoring of business relationships” (transaction monitoring) to intra-group outsourcing only. Other functions such as filtering and KYC may be outsourced. The rationale for this limitation is unclear and may not be primarily driven by privacy concerns.
- The legislative process is not always flawless and may contain gaps or unintended consequences. Laws should not be treated as “sacred.”
- The main barrier to data sharing between banks for monitoring lies more in legal and ethical concerns than in technical feasibility. Ethics should be embedded in legal frameworks.

Alternatives and future outlook (cross-interview themes)

- Banks are exploring Multi-Party Computation (MPC) as an alternative to direct data sharing; MPC allows calculations on distributed data without actually sharing the data. However, MPC is currently energy-intensive and faces scalability challenges for large transaction volumes. Some argue that if MPC works, the law should allow direct data sharing under secure conditions.
- A government-led initiative, such as the model in Germany where a central public authority processes the data, is legally permitted and avoids risks associated with commercial parties. However, this raises questions about citizens’ trust in the government having access to all their transaction data.

These points illustrate the complexity of financial monitoring, the roles of banks and the FIU, and the specific challenges around data sharing and privacy, as exemplified by the TMNL initiative. Standardizing processes remains difficult due to the diversity of institutions and risk profiles.

References

Anthony, N. (2024). 'the right to financial privacy'. *Cato Policy Analysis'*. https://www.cato.org/policy-analysis/right-financial-privacy

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh,
bibinitperiod N. E. (2024). Data privacy laws and compliance: A comparative review of the eu gdpr and usa regulations. *Computer Science & IT Research Journal*, *5*, 528–543. https://doi.org/https://doi.org/10.51594/csitrj.v5i3.859

Betaalvereniging Nederland. (2025). Feiten & Cijfers [Accessed: 2025-06-26]. https://www.betaalvereniging.nl/actueel/feiten-cijfers/

Bhatta, A., Cortes Arevalo, J., Führer, K., Goyal, N., Heerkens, L., Slaats, E., Subramanian, M., van der Voort, H., & Zhauniarovich, Y. (2024). Designing policy relevant research. *Study material for EPA222A*.

Bociga, D., Lord, N., & Bellotti, E. (2024). Dare to share: Information and intelligence sharing within the uk's anti-money laundering regime. *Policing and Society*, 1–20. https://doi.org/https://doi.org/10.1080/10439463.2024.2428735

Brits, H., & Jonker, N. (2023, November). *The use of financial apps: Privacy paradox or privacy calculus?* (Working Paper No. 794) (The views expressed are those of the authors and do not necessarily reflect official positions of De Nederlandsche Bank.). De Nederlandsche Bank (DNB). Amsterdam, The Netherlands. https://www.dnb.nl

Buckley, G., Caulfield, T., & Becker, I. (2024). Gdpr and the indefinable effectiveness of privacy regulators. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyae017

Buhmann, J., Frasconi, P., Giuseppe, N., & Salvatore, R. (2019). Interactive learning. In *Machine learning and knowledge discovery in databases* (pp. 113–127). Springer. https://doi.org/10.1007/978-3-030-13283-5_6

Bunq. (2022, October). The case of bunq vs. dnb: Effectivity vs. dogma [Accessed: 2025-05-21]. https://www.bunq.com/en-nl/blog/the-case-of-bunq-vs-dnb-effectivity-vs-dogma

Centraal Bureau voor de Statistiek. (2023). Bijna 8 op de 10 mensen deden online aankopen in 2023 [Accessed: 2025-04-25]. https://www.cbs.nl/nl-nl/nieuws/2023/49/bijna-8-op-de-10-mensen-deden-online-aankopen-in-2023

Clarcke, R. (1997). What is privacy. *Australian law Reform Comission*.

Claver, C., Khoury, C. E., & Weeks-Brown, R. (2023, December). Financial crimes hurt economies and must be better understood and curbed [Blog post]. https://www.imf.org/en/Blogs/Articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed

Cross, C., Parker, M., & Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: The case of the ashley madison data breach. *International Review of Victimology*, *25*(1), 53–69. https://doi.org/10.1177/0269758017752410

De Nederlandsche Bank. (2025, January). *Cash nog steeds populair in europa, maar gebruik neemt verder af* [Geraadpleegd op 27 mei 2025]. https://www.dnb.nl/algemeen-nieuws/nieuws-2025/cash-nog-steeds-populair-in-europa-maar-gebruik-neemt-verder-af/

European Data Protection Supervisor. (2025). Data protection [Accessed: 2025-05-28]. https://www.edps.europa.eu/data-protection/data-protection_en

Federal Bureau of Investigation. (2025). Cointelpro [Accessed: 2025-06-19].

Ferwerda, J., van Saase, A., Unger, B., & et al. (2020). Estimating money laundering flows with a gravity model-based simulation. *Scientific Reports*, *10*, 18552. https://doi.org/10.1038/s41598-020-75653-x

Financial Action Task Force. (2022, April). Report on the state of effectiveness and compliance with the fatf standards [Accessed: 2025-06-01].

FIOD. (2018). Ing betaalt 775 miljoen vanwege ernstige nalatigheden bij voorkomen witwassen [Accessed: 2025-03-27]. https://www.fiod.nl/ing-betaalt-775-miljoen-vanwege-ernstige-nalatigheden-bij-voorkomen-witwassen/

Fitzpatrick, M., & Lynch, S. (2016, December). *Stopping terror finance: Securing the u.s. financial sector* (114th Congress, Second Session Report). U.S. House of Representatives. https://financialservices.house.gov/uploadedfiles/terror_financing_report_12-20-2016.pdf

Friedewald, M., Finn, R., & Wright, D. (2013, January). Seven types of privacy. https://doi.org/10.1007/978-94-

Gerbrands, P., Unger, B., Getzner, M., & Ferwerda, J. (2022). The effect of anti-money laundering policies: An empirical network analysis. *EPJ Data Sci.*, *11*(1), 15. https://doi.org/10.1140/epjds/s13688-022-00328-8

Hardouin, P. (2009). Banks governance and public–private partnership in preventing and confronting organized crime, corruption and terrorism financing. *Journal of Financial Crime*, *16*(3), 199–209. https://doi.org/10.1108/13590790910971757

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). “It wouldn’t happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Holtzman, D. H. (2006). *Privacy lost: How technology is endangering your privacy* [Hardcover, 352 pages]. Jossey-Bass.

International Monetary Fund. (2025). *Anti-money laundering and combating the financing of terrorism (aml/cft)* [IMF Financial Integrity topic page, accessed 31 May 2025]. https://www.imf.org/en/Topics/Financial-Integrity/amlcft

International Telecommunication Union. (2024). Measuring digital development: Facts and figures 2024 – internet use [Accessed: 2025-06-19].

Jensen, R. I. T., & Iosifidis, A. (2023). Fighting money laundering with statistics and machine learning [Cited by: 12; All Open Access, Gold Open Access, Green Open Access]. *IEEE Access*, *11*, 8889–8903. https://doi.org/10.1109/ACCESS.2023.3239549

Johnston, J., & Gulliver, R. (2022). What are wicked problems? [Accessed: 2025-06-01].

Judge, K., & Kashyap, A. K. (2024, March). *Anti–money laundering: Opportunities for improvement* (White Paper) (WIFPR Working/White Paper). Wharton Initiative on Financial Policy Regulation, The Wharton School, University of Pennsylvania. https://wifpr.wharton.upenn.edu/wp-content/uploads/2024/03/WIFPR-Anti-Money-Laundering-Judge-and-Kashyap.pdf

Ketenci, U. G., Kurt, T., Önal, S., Erbil, C., Aktürko□lu, S., & İlhan, H. Ş. (2021). A time-frequency based suspicious activity detection for anti-money laundering. *IEEE Access*, *9*, 59957–59967. https://doi.org/10.1109/ACCESS.2021.3072114

Ketonen-Oksi, S., Jussila, J. J., & Kärkkäinen, H. (2016). Social media based value creation and business models. *Industrial Management & Data Systems*, *116*(8), 1820–1838. https://doi.org/10.1108/IMDS-05-2015-0199

KPMG Advisory N.V. (2023, August). Krachten gebundeld, naar een effectievere en efficientere invulling vna de poortwachtersrol in nederland [Accessed: 2025-05-31]. https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/sectoren/krachten-gebundeld-markets.pdf

KPMG Advisory N.V. (2024, May). Emerging trends: Navigating the future of the aml compliance landscape [Accessed: 2025-05-25]. https://kpmg.com/nl/en/home/insights/2024/05/emerging-trends-navigating-the-future-of-the-aml-compliance-landscape.html

Labib, N. M., Rizka, M. A., & Shokry, A. E. M. (2020). Survey of machine learning approaches of anti-money laundering techniques to counter terrorism finance. *Internet of Things—Applications and Future*, *114*, 73–87. https://doi.org/https://doi.org/10.1007/978-981-15-3075-3_5

Lichter, A., Löffler, M., & Siegloch, S. (2019). *The long-term costs of government surveillance: Insights from stasi spying in east germany* (ifo Working Paper No. 317). ifo Institute – Leibniz Institute for Economic Research at the University of Munich. https://www.ifo.de/DocDL/wp-2019-317-lichter-loeffler-siegloch-stasi-east-germany.pdf

Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., & Clark, J. (2024, May). *Artificial intelligence index report 2024* (AI Index Report). Stanford University, Stanford Institute for Human-Centered Artificial Intelligence. https://hai-production.s3.amazonaws.com/files/hai_ai-index-report-2024-smaller2.pdf?utm_source=chatgpt.com

McCarthy, P. (2012). Privacy, challenges to [Formerly of Lancaster University, Lancaster, UK]. In *Encyclopedia of applied ethics* (pp. 599–608). Elsevier.

Ministerie van Justitie en Veiligheid. (2024, June). *Kerncijfers politie bij het eerste halfjaarbericht 2024* (Rapport) (Bijlage 1 bij de Kamerbrief "1e Halfjaarbericht politie 2024"). Ministerie van Justitie en Veiligheid. Den Haag. Retrieved June 30, 2025, from https://www.eerstekamer.nl/overig/20240711/bijlage_1_kerncijfers_politie_bij/document3/f=/vmf0jlb2iezl.pdf

Msc engineering and policy analysis (epa) [Accessed 24 June 2025]. (2025). Delft University of Technology. Retrieved June 24, 2025, from https://www.tudelft.nl/studenten/faculteiten/tbm-studentenportal/onderwijs/master/msc-epa

Nederlandse Vereniging van Banken. (2024, April). Nextgen poortwachters - naar een gerichte, proportionele en effectieve aanpak [Position Paper]. https://www.nvb.nl

Netherlands, F. I. U. (2024, June). *Jaaroverzicht 2023* (Annual Report) (Published 28 June 2024; accessed 31 May 2025). FIU-the Netherlands. Zoetermeer, The Netherlands. https://www.fiu-nederland.nl/wp-content/uploads/2024/06/FIU-Jaarverslag-web-2023-T.pdf

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

NOS. (2024). Banken bouwen gezamelijk antiwitwasproject af. *NOS*. https://nos.nl/artikel/2526940-banken-bouwen-gezamenlijk-antiwitwasproject-af

NOS. (2025). Minister heinen: Witwascontrole door banken is vastgelopen. *NOS*.

Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. *Future Generation Computer Systems*, *159*, 161–171. https://doi.org/https://doi.org/10.1016/j.future.2024.05.027

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? together, we can fix it. *Policy Design and Practice*, *3*(1), 73–94. https://doi.org/10.1080/25741292.2020.1725366

Ryngaert, C., & Taylor, M. (2020). The gdpr as global data protection regulation? *American Journal of International Law*, *114*, 5–9. https://doi.org/10.1017/aju.2019.80

Solove, D. (2006). A taxonomy of privacy [Also available on SSRN, working paper No. 667622]. *University of Pennsylvania Law Review*, *154*(3), 477–564. https://ssrn.com/abstract=667622

Solove, D. (2009). *Understanding privacy*. Harvard University Press.

Solove, D. (2025). *On privacy and technology* [Available at SSRN: https://ssrn-com.tudelft.idm.oclc.org/abstract=5159448 or http://dx.doi.org.tudelft.idm.oclc.org/10.2139/ssrn.5159448]. Oxford University Press.

Solove, D. J. (2025). Daniel j. solove [Accessed: 2025-06-05].

Stallings, A. (2024). Balancing privacy and anti-money laundering governance in the era of artificial intelligence. *Security and Intelligence*, *9(1)*.

Strop, J.-H. (2024, June). *Banken bespieden samen je betalingen – illegaal, maar niemand grijpt in* [Geraadpleegd op 1 juni 2025]. Follow the Money. https://www.ftm.nl/artikelen/transactiemonitoring-banken-illegaal

Suzumura, T., Zhou, Y., Kawahara, R., Baracaldo, N., & Ludwig, H. (2022). Federated learning for collaborative financial crimes detection. In H. Ludwig & N. Baracaldo (Eds.), *Federated learning: A comprehensive overview of methods and applications* (pp. 455–466). Springer International Publishing. https://doi.org/10.1007/978-3-030-96896-0_20

United Nations. (2015). Sustainable development goal 16: Peace, justice and strong institutions [Accessed: 2025-05-08].

United Nations Office on Drugs and Crime. (2019, March). *Privacy: What it is and why it is important* [E4J University Module Series — Cybercrime, Module 10 "Privacy and Data Protection", Key Issues section]. Retrieved June 30, 2025, from https://sherloc.unodc.org/cld/zh/education/tertiary/cybercrime/module-10/key-issues/privacy-what-it-is-and-why-it-is-important.html

United Nations Office on Drugs and Crime. (2023). Money laundering - overview [Accessed: 2025-03-27]. https://www.unodc.org/unodc/en/money-laundering/overview.html

Voeten, T. (2025, February 18). Chapter 5: The netherlands as a functional narco-state. In *The devil's drug: The global emergence of crystal meth* (pp. 57–64). Rowman & Littlefield Publishers. https://doi.org/10.5771/9781538198629-57

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

Xu, C., Qu, Y., Xiang, Y., & Gao, L. (2023). Asynchronous federated learning on heterogeneous devices: A survey. *Computer Science Review*, *50*, 100595. https://doi.org/https://doi.org/10.1016/j.cosrev.2023.100595

Xu, Q., Wang, S., & Tao, Y. (2025). Enhancing anti-money-laundering detection with self-attention graph neural networks. *Proceedings of the International Conference on Management, Economic and Sustainable Social Development (MESSD 2025)*, *213*, 01016. https://doi.org/10.1051/shsconf/202521301016