|  |  |
| --- | --- |
|  | |
| Data Management–Assessment 1  TU060 : Ethics, Data Governance, and Data Privacy Issue in Watchlist Management Software (Commercial) | |
|  | |
| Ciaran Finnegan – Part Time – First Year 2021/2022  MSc in Computer Science (Data Science)  Student No : D21124026  1/3/2022 |  |
|  |  |

Table of Contents

1 Introduction 3

1.1 What is Commercial Watchlist Management? 3

1.2 WLM: The Key Ethical and Legal Issues? 4

2 Product: BAE Digital Intelligence NetReveal WLM 6

2.1 General Overview 6

3 First Principles Ethics Test: Watchlist Management 7

3.1 Purpose of the test 7

3.2 Outcome of the test: Watchlist Management 7

3.3 Other Ethical Theories: Watchlist Management 11

4 NetReveal WLM: Data Management Approach 12

4.1 BAE Systems D.I. Company Policy on Data Governance and Data Privacy 12

5 Conclusions 14

5.1 Conclusion 1 14

5.2 Conclusion 2 14

6 References 15

# Introduction

## What is Commercial Watchlist Management?

The majority of Financial Intuitions operating in the modern global marketplace are bound by compliance regulations and/or legislation to prevent *money-laundering* being transacted through their systems.

A simplistic definition of *Anti-Money Laundering* (AML) practices in a Financial Institution could be determined as any integrated set of processes and automated system to detect, prevent, and report *restricted* activity in a financial network.

The term ‘restricted’ can be considered not just suspected criminal or terrorist related transactions, but also activity by ‘Politically Exposed Persons’ (P.E.P) who may be the subject of multi-government sanctions.

A major characteristic of AML systems is the use of various internal and external **Watch Lists**. These are data stores that identify specific individuals or companies and are used to influence decisions made by financial institutions.

This infographic from **Chartis** **Research**, a leading provider of research and analysis for financial risk technology, describes the very high process, and the dependency on Watch Lists and Watch List Management (WLM) systems.

Text

Description automatically generated

This report focus on the use of these Watch Lists by Financial Intuitions in AML systems, and the associated data management challenges.

Section 1.2 describes the general ethical/legal issues in the AML/WLM domain.

Section 2 provides a more in-depth view of a vendor product operating in this space – the BAE Systems Digital Intelligence **NetReveal** WLM system.

## WLM: The Key Ethical and Legal Issues?

Taking GDPR regulations as an example, inclusion of an individual on a Watch List is, by definition, the recording of special category data.

In general, the use of Watch Lists in AML systems is permitted by international law and controlled by a number of governmental (and non-governmental authorities). For example, Article 6 of GDPR legislation includes the basis for collection and processing personal data for AML purposes.

In fact, it would be more correct to say that Financial Institutions are obliged by law, in most cases, to regularly scan their client base and transaction records and proactive detect money-laundering activities.

However, the implementation of these Watch List systems generates a number of data management challenges, such as those described below.

### WLM: Ethics

It is good for society as a whole to prevent Financial Institutions from facilitating ‘immoral’ business transactions, and to punish those institutions that deliberately, or carelessly, allow such practices.

However, the use of Watch Lists often deliberately run contrary to many of the recent safeguards introduced for individuals and how personal data is stored.

It goes without saying that individuals rarely ask to be added to a Watch List or give their consent.

Manu individuals may be unaware of their presence on a Watch List and legislation such as GDPR or the Irish Data Protection Act 2018 give very limited options to uncover inclusion on an EU Watch List, let alone provide an option to be removed.

In addition, name matching is not always an exact science. Therefore, companies must constantly ensure that ‘Fuzzy’ matching algorithms minimise both false positive and false negative matches.

### WLM: Data Governance

WLM systems developers and controllers/processors must ensure (from the C-level downwards) that established, continuous, and evolving policies are in place to keep Watch Lists up to date.

Every FI must have named staff that can interpret why internal (or vendor) WLM software flagged an individual or transaction against a given Watch List.

A named individual, or group of individuals, within an FI must hold responsibility for the reporting of suspicion activity to the relevant regulatory authority. This group must also be aware of the penalty for the FI for failure, by inaction or inability, to comply with these regulations.

### WLM: Data Privacy

Access to Watch Lists must be restricted to those with appropriate clearance both within a Financial Institution, and within the vendor company supplying WLM software.

Watch List data must not be used outside of the intended purpose of preventing money laundering or the funding of illegal activity (a Use Limitation Principle applies).

As mentioned above. AML processes will use Watch Lists in ways that differ from the rights that individuals would be guaranteed, or expect, in other domains. For example, GDPR Article 17 contains legislation on the ‘*right to be forgotten*’. However, the EU’s 4AMLD takes precedence and an FI must record history of suspected suspicious activity for five years. Also, GDPR allows data to be preserved to comply with a ‘legal ruling’, which make it difficult for an individual to be removed from an EU based Watch List.

# Product: BAE Digital Intelligence NetReveal WLM

## General Overview

The BAE Systems D.I. NetReveal (NR) AML/WLM solution is one of the key vendors providing an offering in this compliance space for Financial Institutions. *(*[*https://www.baesystems.com/en-financialservices/solutions/banking-compliance*](https://www.baesystems.com/en-financialservices/solutions/banking-compliance)*)*

**Text

Description automatically generated with medium confidence**

The product is aimed at Tier-1 Financial Institutions that generally favour an on-site deployment on company premises. The client base for this product remains relatively resistant to cloud-based solutions, so the NR WLM system generally fits into an existing ecosystem of in-house company applications that monitor daily business transactions.

The primary geographical locations for NR WLM deployments are in North America, EMEA and the Asia Pacific region.

Taking the example of EU based clients, Article 28 of GDPR states that data controllers (Financial Institutions) must appoint data processors, like BAE Systems, who can offer and demonstrate “sufficient guarantees” of GDPR compliance – in the area of AML/WLM in this case.

Since the NR system processes personal data (in Watch Lists) for each client, the GDPR compliance guarantees must be set out in advance in the product terms of service agreements.

It is important to note that NR AML/WLM solutions, in common with most similar vendor solutions, do not limit name matching to just ‘*names*’. Other identifiers can, and must, be used in the matching process, for example DOB, country of birth, names of known associates, etc.

The NR WLM name screen process provides all the functionality, and associated challenges as described in Section 1of this document. A key characteristic of the NR system is that it must perform the name matching as effectively as possible, but *the actual end result of this process is dictated by client themselves*. This can result in a decision process to general a suspicious activity report (SAR), flag a transaction for investigation, or even to automatically block a payment from being authorised.

# First Principles Ethics Test: Watchlist Management

## Purpose of the test

A First Principles Ethical Test for the NetReveal Watch List Management product will attempt to answer this question;

* *Do the WLM processes facilitated and supported by this product contribute positively to ‘the good’, or the positive preservation of human rights?*

We have already seen in this report that many of the usual data rights and expectations that individuals would have under legislation such as GDPR is heavily tempered by complimentary legislation that seeks to prevent money laundering (or related) criminal activity within a Financial Institution.

The test seeks to determine if the correct balance of ethics applies, and what the associated risks may be.

## Outcome of the test: Watchlist Management

### Does it preserve or enhance human dignity?

Section 1.2.1 of this document makes a brief reference to the challenge faced by all WLM products, including NetReveal, that they must match a name on a new transaction as accurately as possible against a published Watch List.

(In the supporting PowerPoint presentation to this report there are some examples of these types of challenges and the impact they can have).

The need for AML systems to prevent crimes that will have a determinantal impact on society is described in Section 3.2.4 below. However, a false match against a Watch List can cause an unfair disruption in service, which can range from a mild delay to outright refusal. For example, a legitimate SEPA transfer for payment of goods may be blocked because the individual has a very similar name and profile to an exposed person on a given Watch List. Stories of an innocent party names *O. Bin Laden* being unable to transaction legal business affair internationally are not unknown.

The NR WLM product employs an algorithm that works as intensively as possible to avoid such ‘false positive’ situations with Watch List matches. To the credit of the vendor, ongoing refinement in this process is a key element in the product roadmap.

Accidental matches can, and do, happen but the product works to eliminate these as much as possible preserve the entitlement to fair treatment for honest individuals using a Financial Intuition for business transactions.

### Does it preserve the autonomy of the human?

It is probably fair to say that there are few individuals who would actually consent to inclusion on a Watch List, but this is a choice that is deliberately denied to them.

If you take the Irish Data Protection Act 2018 as just one representative example, Section 60 lists many clauses under which an individual can be prevented about finding out about their inclusion on a Watch List, let alone be granted a request to be removed.[]

Reasons to refuse such confirmation/deletion requests from an individual can be;

* Ongoing criminal investigations
* National security or other threats to public safety
* Economic obligations to the European Union

However, legislation such as GDPR does strongly recommend that Personally Identifiable Information (PII) on Watch Lists is not excessive and is limited to a reasonable set of identifiers.

There are strong guidelines from the European Data Protection Supervisor (EDPS) on what constitutes a ‘reasonable’ set of identifiers. The NR WLM product follows these principles by not using the following types of characteristics in the name matching process;

* Ethnicity
* Sexual Orientation
* Religion

The product scores well in intent in this part of the test, but in practice it falls a little short. Passport names and nationality can usually infer ethnicity. The WLM name matching process also tracks known associates, who may be facilitating corruption or tax avoidance with a PEP. It is not unheard of for politicians in certain regimes to transfer funds illegally through wives and mistresses, and hence strongly imply the likely sexual orientation.

On balance the product works as well as might be expected to obey the letter of the law, but may occasional oversteps the bounds of what the EDPS considers fair in terms of business WLM.

### Is the processing necessary and proportionate?

The necessity of WLM systems in Financial Institutions is mandated, in almost all jurisdictions, by law. Therefore, the necessity for such Watch List processing is clear, and companies can be fined severely if appropriate systems are not in place.

Again, this overlaps with the points in Section 3.2.4 below, as the purpose of these AML/WLM process is to reduced criminal activity which has a negative impact on society as a whole/

In terms of ‘proportionate’ the product largely passes this section of the test because;

* The NR WLM processes only explicitly use a recommended sub-set of PII data in the name matching process. However, Section 3.2.2 does call out some short coming in this approach.
* Watch Lists are within a Financial Institution as soon as a Watch List provider issues a notification of a change. The NR WLM application has a series of well tested API routines to automatically pull down these revisions and apply into production systems as quickly as possible. Therefore, name matching never takes place against ‘stale’ data and the actions decided upon by the Financial Institution are always based on the most current Watch List content.

### Does it uphold the common good?

This is arguably the biggest driver for the implementation of WLM systems such as NetReveal and the matching of named individuals (or companies) against the data stores of PII listed in published Watch Lists.

As we see in Section 3.2.2 an individual on a Watch List can have very little say about their personal information being part of these particular data stores. However, global society enforces these AML process to reduce the following activities;

* **Illegal transfer of criminal funds**. Activity such as the sale of narcotics or human trafficking are an obvious societal ill. Any reasonable person would deem these practices and ethically repugnant.
* **Funding of terrorist activity**. This is an obvious threat to public safety.
* **Activities by P.E.Ps (Politically Exposed Persons).** Recent studies show that Africa loses nearly as much in the illegal expatriation of funds and non-payment of taxes, as it takes in through international aid. Therefore, the funding of public services in some countries is negatively impacted by the selfish actions of corrupt officials and such be prevented by the global Financial Markets. The restriction of financial activity by political figures close to the Putin regime in the aftermath of the invasion of Ukraine is another example of a desirable and ethical response to war crimes.

NR WLM scores well here in that is an effective tool in policing good financial practice.

### Does the outcome violate any of these four points? Can the risk be mitigated?

A..

**Graphical user interface, application

Description automatically generated**

## Other Ethical Theories: Watchlist Management

As

# NetReveal WLM: Data Management Approach

## BAE Systems D.I. Company Policy on Data Governance and Data Privacy

### NR: Data Governance Characteristics

* The client data and transactions being monitored by a Financial Intuition for AML purposes is never transferred to an external hosted services for name matching by NetReveal. Watch List data is imported *into* the Financial Services systems by NR.
* Every time the NR WLM application matches a name against a Watch List it generates a ‘score’ that reflects system confidence that the match is correct. These algorithms frequently use ‘Fuzzy’ matching techniques to catch misleading variants in names, such as the use of abbreviations or ethnic spellings. Alerts for investigators will be generated based a given score threshold, and this will determine the eventual response.
* It is essential that the Watch Lists in use by the NR WLM deployment within a client are kept as up to date as possible[x]. The NR product uses a number of inbuild API routines to download updates from providers such as Dow JOE, BOE, etc as soon as they are available.

### NR: Data Ethics + Privacy Characteristics

* Every new NR product release delivers refinements to name matching algorithms to reduce false positive and false negative results. This cycle of innovation is essential because:
  + *A false positive result generates unnecessary, and expensive, workloads for company investigators and may unfairly block or delay a service to a customer. For this reason, Tier-1 Financial Institutions often have a global workforce of AML/Fraud investigators that number in the tens of thousands. False red flags for AML can be very labour intensive to assess manually.*
  + *The much greater ethical concern is a false negative that fails to capture restricted activity for which the Financial Institution is legally, and morally, bound to intercept. Aside from the ethical imperative to intercept illegal transfer of funds, the fines for a company that fails to implement reasonable AML safeguards can run into the millions (or billions) of Euros.*
* In line with GDPR recommendations, NR WLM algorithms do not include ethnicity, sexual orientation, or religion in the name matching process.
* GDPR legislation requires that access to PII is restricted to only those with a legitimate need to process the data. It is the subject of current debate that this may restrict the activity of software engineers and testers who develop NR WLM software. This is an EU industry wide challenge, for which a definitive ruling has not yet been made.

### NR WLM: Data Management Recommendations

Looking over the brochure ware provided by BAE Systems, along with general industry and ethical concerns about the processes of commercial Watch List management, I would suggest the following recommendations;

* Fuzzy name matching algorithms have become increasingly sophisticated in the last decade, but the rate of false positives generated by systems such as NR WLM is a constant concern for Financial Institutions. Advances in Machine Learning techniques for scoring name matches are an emerging trend in this area, and the NR product needs to continue to incorporate these types of innovations.
* GDPR critics have complained that applications like NR make it relatively easy to infer restricted PII data such as ethnicity or sexual orientation from their WLM processes. There is a balancing act involved in ensuring that the criteria for a name matching score is clearly understood, but not also allowing peripheral assumptions to be made about the individual being investigated. This is a requirement that NR WLM Product Owners should attempt to address in later versions of the product.
* The NR WLM application, along with supporting deployment consultants and services engineers, act as a processor of Watch List data but do not control the end result of the name matching process. This is an arrangement that must remain in place to avoid ambiguity around who is ultimately responsible for the final decisions made by an AML process.
* Although GDPR does allow a Financial Intuition to configure the NR system to make automatic decisions based on a Watch List match, it must always be clear that the client company (and named people within that company) are responsible for the actual end decisions made.
* The content of the Watch Lists, including supported internal watch lists, must remain the responsibility of the provider – not the vendor (NR in this case). This ensures there is no ambiguity as to where the responsibility for the inclusion of individuals on a Watch List resides.

# Conclusions

## Conclusion 1

The

## Conclusion 2

The

# References