Enhancing the construction of attacker personas in cybersecurity software designs using case law-based facts.

ILESANMI, O., FAILY, S., NICHO, M. and MCDERMOTT, C.

2024

Enhancing the Construction of Attacker Personas in Cybersecurity Software Designs using Case Law-Based Facts

ABSTRACT

Thwarting potential attackers is always at the heart of cybersecurity software designs. This interdisciplinary paper in computing science and law investigates the possibility of building attacker personas through reliance on case law facts. To combat the threat of cybercrime, software engineers, cybersecurity professionals and law enforcement agencies across the globe are turning to attacker profiling. A persona is a model which is created based on archetypical user behaviour and it identifies patterns or common traits of users via data. Personas, which are then identified from collated and analysed data, provide insight into behaviours and characteristics of cybercriminals, namely convicted deviants who attack government, corporate and individual or family networks. By creating personas for both attackers and victims of cybercrimes, software engineers may so identify the type of person or organisation who is likely to be a cybercriminal and those likely to be targeted for abuse.

Similarly, in law, attacker and victim profiles provide specific characteristics of an attacker or victim. Facts, which are put together by trial courts in case law and upon which judges apply legal principle to make decisions, could also serve as data for the building of personas. The study accordingly aims at determining whether, and to what extent, an attacker persona can be created using case law facts. Our research in law and computing science demonstrates that, while the idea of profiling offenders is not new, understanding profiles for the purpose of building personas using case law-based facts is novel. And, by introducing case law as complementary method for building personas, this paper offers for a cross-disciplinary and unique approach that makes personas building easier for cybersecurity software designers or engineers.

In support of arguments that case law facts could complement persona building models that are known to software scientists or designers, the first section of the paper explains key terms, concepts, and reviews methodological approaches as understood operationally. Second section reviews the literature. Third is a review of personas building method of using case law, expounding its scopes and limits through the lens of American Legal Realism that explores the relationship between decision making, applicable principles and relevant facts. To illustrate reliability of case law facts for offender profiling, what follows are analyses of sample cases including *McKinnon v Government of the United States of America*, *Love v United States* and *Regina v Steffan Needham*. Finally, the study revisits the central question on the usefulness of case law for building attacker personas which engineers could use in designing software for thwarting future attacks.

1) INTRODUCTION

Cybercrime is "any illegal behaviour committed by means of, or in relation to, a computer system or network including such crimes as illegal possession of and offering or distributing information by means of a computer system or network".[1] With 90% of UK households and individuals having digital access, the risk of cyber-attacks is heightened due to the "interconnected nature of networks, systems and devices used by organisations and individuals".[2] For example, in the UK, between 2021 and 2022, 39% of businesses identified a cyber-attack[3] and 31% of businesses and 26% of charities within the group of organisations reporting cyber-attacks estimating they were attacked at least once per week[4]. Therefore, cybercrimes present a risk to individuals, and businesses. National security is also at risk, with cyber threats being assigned a 'Tier One' threat status in the 2010 National Security Strategy and reaffirmed in 2015.[5]

To combat the threat of cybercrime, software engineers, law enforcement agencies and cybersecurity professionals have turned to attacker and victim profiling. A persona is a model of archetypical user behaviour based on patterns or common traits of users developed from data.[6] Personas, which are grounded in analysed data, provide insight into behaviours and characteristics of cybercriminals, who attack government, corporate or individual or family networks.[7] By creating personas for both attackers and victims of cybercrimes, the type of person or organisation that is likely to be cybercriminal and those likely to be targeted as a victims may be identified.

Similarly, in law, attacker and victim profiles provide detailed and specific characteristics of attackers or victims. *Facts*, which are evidence put together by trial courts in case law and upon which judges apply legal principle to make decisions, could also serve as data for the building of personas.[8] While the practice of profiling attackers is not new, this paper offers an entirely new interdisciplinary approach to the development of attacker and victim personas for cybersecurity. By analysing case law, we present a novel approach that complements designers' models for persona creation.

---

[1]Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 172.

[2] UK Parliament, 'Delivering the National Cyber Security Strategy' (2019) < Cyber security in the UK - Committee of Public Accounts - House of Commons (parliament.uk)> accessed 7 June 2022

[3] Department for Digital, Culture, Medica and Sport, 'Cyber Security Breaches Survey 2022' (Gov.UK, 30 March 2022) < Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk)> accessed 4 April 2022.

[4] Department for Digital, Culture, Medica and Sport, 'Cyber Security Breaches Survey 2022' (Gov.UK, 30 March 2022) < Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk)> accessed 4 April 2022.

[5] Mike McGuire and Samantha Dowling. 'Cyber Crime: A Review of the Evidence – Research Report 75: Summary of Key Findings and Implications' (2013) at p4.

[6] Plinio Thomaz Aquino Junior and Lucia Filgueiras, 'User Modelling with Personas' (2005)

[7] The first one being the focus of cybersecurity, whereas the latter is mostly the focus of cybercrime.

[8] See generally Lee Loevinger, "Facts, Evidence and Legal Proof" (1958) 9 Case Western Reserve Law Review 2, 154 Available at Facts, Evidence and Legal Proof (case.edu) accessed 6 August 2022. Trial and appellate court judges explain their decisions on lawsuits usually through written determinations, sometimes described as case laws. The formats of case law allow judges to spell out the decision; the main questions before the court; as well as principles or rules that it applied to the evidenced-based collated facts. Case law facts account for the "who, when, what, where, and why" of the dispute before courts. Consisting of evidenced-based account and background of lawsuits, the facts are then presented within the judgements. Being important information affecting the outcome of legal dispute, case law-based facts are no-less material. Software scientists, it is argued, could consider generating complimentary data for building personas from case law-based facts.

This interdisciplinary study in computing science and law therefore aims at determining whether, and to what extent, an attacker persona can be created using case law facts. Our research in law and computing science demonstrates that, while the idea of profiling offenders is not new, understanding profiles for the purpose of building personas using case law-based facts is novel. And, by introducing case law as complementary method for building personas, this paper offers a route to for a cross-disciplinary and unique approach to enable cybersecurity software designers or engineers to strengthen existing personas .

Structurally, focussing on the possibility of creating attacker personas through case law facts, the study starts with a review of key concepts, including the four-step hybrid profiling model and the six profile identification metrics. These models are all used to identify the attacker in the three cases evaluated, and concern cyber-attacks on the state, companies, and individuals. The sample cases include *McKinnon v Government of the United States of America*, *Love v United States* and *Regina v Steffan Needham*.

The second section reviews relevant literature and the methodology. This provides an opportunity to review the introduction of personas, for attackers, to software design. It also explores profiling techniques, which focuses on attackers.

Third is a review of personas building methods using case law, expounding its scopes and limits through the lens of American Legal Realism as it considers the relationship between decision making, applicable principles and facts derived from study of relevant case law. This provides an opportunity to study closely explicit facts as well as useful implicit data, which case law provides. A doctrinal legal research approach is, by extension, used to determine material facts.

In section four, to determine reliability of case law for offender profiling, what follows are analyses of sample cases. It carries out an examination of case law, which specifically includes *McKinnon v Government of the United States of America*, *Love v United States*, and *Regina v Steffan Needham*, to identify patterns and behaviours in relation to cybercrime attackers and victims.

Section five revisits the central question regarding the suitability of case law for building attacker personas, which engineers might use in designing software for thwarting future attacks. American legal realism, as a theory, provides the tool to determine usefulness of case law facts, analysing strengths and weaknesses.

Meanwhile, included in this Introductory section is an explanation (overview) of key methods, terms and concepts as understood operationally. Suitability of case law facts and exploration of attacker personas is examined through extensive desk research using primary and secondary sources within law. Before studying key terms and concepts, an overview of existing approaches and relevance of jurisprudence to persona building is considered in brief. This provides an opportunity to explain attacker profiling within law, with specific reference to cybercrime, and the use of Warikoo's method for constructing attacker personas.

Between the Existing Models and Case Law Facts: Recent work by Caroline Moeckel[9] explores the idea of building personas for attackers from an information security perspective; this paper considers the merit of using case law to construct such personas. While the focus is on the relevance of case law to

[9] Moeckel, Caroline. "Modelling digital banking attackers: attacker-centric approaches in security." PhD diss., Royal Holloway, University of London, 2020.

the construction of personas, models for profiling cybercriminals are contemplated: First, Arun Warikoo's[10] identification metrics for cybercriminals, and second, Moeckel's proposed methodology,[11] both coming from the background of computing and information security. Third, our own study explores building attacker personas through case law with a focus on American Legal Realism (ALR): as shall be made apparent, ALR is a doctrinal and methodological approach championed by academics John Chipman Gray (1839-1915) and Karl Llewellyn (1893-1962), and judges Oliver Wendell Holmes (1841-1935) and Jerome Frank (1889-1957) among others. In considering the foregoing personas building perspectives, this study appreciates that, although backgrounds or context in which they apply may vary, interests are similar -with all being interested in how to establish facts about an ongoing reality. Warikoo's approach, which seems more prevalent, requires the collection of data on various factors including the attacker's signature, attack method, level of motivation, capability, attack severity, and demographics.

Warikoo's proposed methodology for profiling cybercriminals[12] is also important related work. Warikoo provides six profile identification metrics; these can be used to identify an attacker. It is important to examine the work available on profiling within cybercrime, especially attackers, as one hypothesis of this work is that to understand a victim persona, it is necessary to profile the attacker. However, Warikoo has no legal background. Hence, his work does not base the proposed identification metrics on case law whereas our work applies Warikoo's metrics to three cases to determine whether case law provides the requisite information and, ultimately, whether case law can facilitate persona creation and use. This provides the interdisciplinary insight lacking in Warikoo's work. Further, Warikoo solely focuses on attackers whereas our work focuses on attackers and, to a certain extent, victims, providing a more balanced view. Thus, as Warikoo does not answer the question of whether case law can be used to create a persona of a victim of cybercrimes, our work is unique and presents a novel outlook on the ways in which personas can be built for cyber security purposes.

While Warikoo focuses on attacker personas, Whitty presents a study on victims of cyberscams.[13] Whitty found that certain characteristics and behaviours of victims corresponds with the type of cyberscam they would most likely be a victim to. This is important as it confirms that profiling is an established tool for cybercrimes and that victims of cybercrimes can be profiled. However, Whitty's article specifically examines cyberscams, which is narrower than the crimes examined in this work and Whitty solely focuses on individual victims. This work focuses on cyber security breaches, with victims that encompass states, companies, and individuals Furthermore, while Whitty does not use case law to construct personas, our work does.

American Legal Realism must then be explored to understand case law facts and its limits.[14] It is concerned with the way law is made and questioning a) how rules and facts are determined as well as b) how legal principles are mechanically applied by formalists to seemingly uncontroversial facts. Leiter provides a detailed overview of the concept of American Legal Realism. He details that the basis of the concept of American Realism is that the law is formed by the rules laid down by judges when

[10] Warikoo, Arun. "Proposed methodology for cyber-criminal profiling." Information Security Journal: A Global Perspective 23, no. 4-6 (2014): 172-178.
[11] Moeckel, Caroline. "Modelling digital banking attackers: attacker-centric approaches in security." PhD diss., Royal Holloway, University of London, 2020.
[12] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172.
[13] Monica Therese Whitty, 'Is There a Scam For Everyone? Psychologically Profiling Cyberscam Victims' (2020) European Journal on Criminal Policy and Research 26:399.
[14] See generally Lee Loevinger, "Facts, Evidence and Legal Proof" (1958) 9 Case Western Reserve Law Review 2, 154 Available at Facts, Evidence and Legal Proof (case.edu) accessed 6 August 2022.

deciding on a case in the court and such a judge's decision is primarily based on stated and implied facts of the case.[15] This practice suggests that case facts are vital and thus can be relied upon to build personas. Leiter usefully supports the basis of this work and highlights the importance of case law. The focus of the article, however, is the theory of American Legal Realism. Whereas the present work applies American Legal Realism principles to cybercrimes in determining whether case law can be relied upon to build personas, Leiter does not contemplate application of the theory to cybercrime cases.

Meaning of Cognate Terms and Concepts: An attacker may well be appreciated in relations to the nature or reality of a victim. In law, a victim is an entity or individual who has "suffered harm including physical, mental or emotional harm or economic loss directly caused by a criminal offence".[16] Thus, there must be 1) harm and 2) the harm must be caused by a criminal offence. In this research, criminal case law, rather the civil case law, is analysed, as these criteria are met. This is because for an incident to progress to a criminal court case, the police and especially the court must be satisfied that a criminal offence occurred.[17] Further, the cases examined within this work highlight the harm caused by the cybercrimes, most of which is financial harm. A wider definition of a victim in the Cambridge Dictionary is "someone or something that has been hurt, damaged, or killed or has suffered because of the actions of someone or something else".[18] When a victim's profile or persona is discussed throughout this work, a victim is defined as above.

The focus of this paper, however, is not on victimhood or the victims themselves, but rather on the attackers as perpetrators or offenders of cybercrime: 'someone who has committed a crime or a violent or harmful act.'[19] A perpetrator therefore can in the jural relation be posited, and by differentiation, in the jural relation on the other side of the victim, having committed the harmful act. Throughout this work, the term 'perpetrator' or 'attacker' is used interchangeably.

Case law generally refers to the decision of judges in court cases and, in the case of this paper, the decisions of judges especially in criminal court cases.[20] These decisions are based on whether the accused, the person who allegedly committed a crime, is guilty of the crime. Case law is accordingly about a judge's written decision, which provides information on a) the *facts* of the case, b) the statute (if any) applied, c) the court's decision, and d) the sanction applied. [21]

While the term "attacker personas" and "attacker profiles" are used interchangeably, they differ slightly from a cybersecurity context. The aim of cyber threat actor profiling is developing profiles, which are based on record of past attacks and establishing profile that would represent or reveal and attacker's profile.[22]Attacker Personas are behavioural specifications of archetypical attackers of a

[15] Brian Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005).
[16] 'Code of Practice for Victims of Crime in England and Wales' (2021) < Code of Practice for Victims of Crime in England and Wales (Victim's Code) - GOV.UK (www.gov.uk)> accessed 30 May 2022
[17] My Gov Scot, 'The Decision to Take a Case to Court' (*mygov.scot,* 25 January 2018) < The decision to take a case to court - mygov.scot> accessed 30 May 2022.
[18] Cambridge Dictionary <VICTIM | meaning in the Cambridge English Dictionary> accessed 5 April 2022
[19] Cambridge Dictionary <https://dictionary.cambridge.org/dictionary/english/perpetrator> accessed 1 June 2023
[20] Emily Finch and Stefan Fafinski, Legal Skills (7th edn, Oxford University Press 2018) 85.
[21] See generally Lee Loevinger, "Facts, Evidence and Legal Proof" (1958) 9 Case Western Reserve Law Review 2, 154 Available at Facts, Evidence and Legal Proof (case.edu) accessed 6 August 2022.
[22] Skopik F, Pahi T. Under false flag: Using technical artefacts for cyber-attack attribution. Cybersecurity. 2020 Dec; 3:1-20.

system.[23] Understanding attackers allow us to generate attacker profiles, known as attacker personas, which can help law enforcement agencies to design effective countermeasures to improve cyber defence initiatives.[24] Matching an attacker profile to the signature of the offence to have an idea of the type of person who committed it will minimize uncertainty at three dimensions, namely tactical, operational, and strategical since human lives and the security of the state may depend on correctly ascribing agency to an agent.[25] Thus, it is necessary to understand, or at least model, their behaviour to effectively counter potentially decisive and skilled attackers.[26]

This work focusses on personas of attackers although victimhood is, to a lesser extent, considered. The work also contributes to the discussion on whether case law can aid in developing personas in the context of cyber security. To do so, the facts provided on the victim and attacker and in the context of a legal cyberattack court cases are discussed. Similarities between cases are identified to determine whether building a persona is possible. Focusing on what is law and reported cases might also help in the future given the seemingly practical theme of this article. It must however be mentioned that this study attempts a more theoretical engagement with a number of reported cases in Section 4 below.

2) A REVIEW OF THE METHODOLOGICAL APPROACH(ES)

Various literature is explored throughout this work to establish that the use of personas helps in identifying and allowing for a better understanding of cybercriminals and victims of cybercrime. It seeks to explore usability and possible limits of case law facts, which it tends to review from the lens of American legal realism. This section therefore considers other models which software engineer use, reviewing the key nature and characteristics.

A) Personas and Attacker Personas

Personas were introduced by Cooper in 1999 to address the issue of technology being designed without real users in mind.[27] They are hypothetical archetypes of users that are employed throughout the design process. Over time, a body of work on “attacker personas" has also developed. Aucsmith et al. proposed "threat personas" in 2003, but provided no guidance on attacker persona creation or data sources was provided.[28] Steele and Jia proposed "anti-personas" and "anti-scenarios" in 2008 based on assumptions about attackers,[29] while Atzeni et. al., recommended an approach close to assumption personas using open-source intelligence data combined with third-party attacker

[23] Atzeni A, Cameroni C, Faily S, Lyle J, Fléchais I. Here's Johnny: a methodology for developing attacker personas. In2011 Sixth International Conference on Availability, Reliability and Security 2011 Aug 22 (pp. 722-727). IEEE.
[24] Brynielsson J, Franke U, Tariq MA, Varga S. Using cyber defense exercises to obtain additional data for attacker profiling. In2016 IEEE Conference on Intelligence and Security Informatics (ISI) 2016 Sep 28 (pp. 37-42). IEEE.
[25] Rid T, Buchanan B. Attributing cyber-attacks. Journal of strategic studies. 2015 Jan 2;38(1-2):4-37.
[26] Brynielsson J, Franke U, Tariq MA, Varga S. Using cyber defense exercises to obtain additional data for attacker profiling. In2016 IEEE Conference on Intelligence and Security Informatics (ISI) 2016 Sep 28 (pp. 37-42). IEEE.
[27] Cooper A. The inmates are running the asylum. Vieweg+ Teubner Verlag; 1999.
[28] Shostack A. Threat modeling: Designing for security. John Wiley & Sons; 2014 Feb 12.
[29] Steele A, Jia X. Adversary Centered Design: Threat Modeling Using Anti-Scenarios, Anti-Use Cases and Anti-Personas. In IKE 2008 Jul 14 (pp. 367-370).

taxonomies.[30] Tariq et al. aligned their attacker types for organized cybercrime with the work of Atzeni et al. and emphasised storytelling and narratives in their personas, which were detached from a specific context.[31]

Work on attacker personas remains limited but derives from user-centred design research on personas and is strongly influenced by key works and authors. Previous work highlighted the importance of user-centred design methods for building personas in the context of attacker personas, establishing them as a distinct variation of persona. For example, Faily & Fléchais emphasised the importance of grounding personas in data and preferred structured, logical validation, and documentation strategies.[32] Here grounded theory was used to code a small number of interview transcripts with expert users and stakeholders. The aim is to validate the proposed personas through a three-step approach: summarizing propositions and core concepts from the grounded analysis, enumerating characteristics such as backing, modal qualifier, and possible rebuttals (using Toulmin's model of argumentation) related to all claims supporting each persona, and finally, writing supporting persona narratives.

B) Profiling Techniques

Criminal profiling is an investigation tool available for law enforcement agencies to identify attackers. This tool analyses crime scene behaviours to aid in identifying "major personality, behavioural and demographic characteristics of an offender". This creates a profile consisting of characteristics likely to be shared by those who commit a certain type of crime.[33] Ultimately, this aids in creating or narrowing the potential suspects based on whether there are links between the crime committed and the characteristics of attacker s who commit such crimes.[34]

Offender profiling is not a novel. In the late 1880s, one perpetrator, known as Jack the Ripper, was linked to the murder of five people due to unique and signature similarities between the attacks; each victim was a white, female prostitute between 24 and 45 years old, the murders took place within a mile of each other, the victims' throats were cut and their bodies were mutilated in an unusual manner, with at least three having their internal organs removed.[35] Thus, patterns and characteristics were identified. It was thought the attacks were pre-planned and organised, and the offender was a

[30] Atzeni A, Cameroni C, Faily S, Lyle J, Fléchais I. Here's Johnny: a methodology for developing attacker personas. In2011 Sixth International Conference on Availability, Reliability and Security 2011 Aug 22 (pp. 722-727). IEEE.
[31] Tariq MA, Brynielsson J, Artman H. Framing the attacker in organized cybercrime. In2012 European Intelligence and Security Informatics Conference 2012 Aug 22 (pp. 30-37). IEEE.
[32] Faily S, Flechais I. Persona cases: a technique for grounding personas. In Proceedings of the SIGCHI conference on human factors in computing systems 2011 May 7 (pp. 2267-2270).
[33] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 173
[34] Bryanna Fox and David Farrington, 'What have we learned from offender profiling? A systematic review and meta-analysis of 40 years of research' (2018) Psychological Bulletin 144(12) 1247, at 1247
[35] Robert D. Keppel, Joseph G. Weis, Katherine M. Brown, Kristen Welch, 'The Jack the Ripper murders: a modus operandi and signature analysis of the 1888-1891 Whitechapel murders' (2005) Investigative Psychology and Offender Profiling 2(1) at 1.

male who liked to control their victim and felt invincible. This was suggested by leaving the victims on display in (often) public places once murdered.[36]

The use of profiling has since extended from murders to almost all types of crime, with many studies focusing on cybercrimes. Profiling aids in identifying potential victims and attackers but also potential motivators for cybercrimes. Like profiling in law, personas are built in the security field to "describe archetypical users of interest to designs" and identify "relevant behaviours and perceptions" of users of data.[37] Thus, profiling in law is like personas built for cyber security purposes.

C.) On Profiling of the Attacker

Central to arguments on attacker profiling is that the "characteristics of an offender can be deduced by a careful and considered examination of the characteristics of the offence".[38] The same can be said about profiling victims. Therefore, before discussing attacker profiling, victim profiling must be mentioned in brief. Whitty conducted a study on the victims of cyber scams and discovered that individuals with impulsive and neurotic tendencies are more susceptible to being scammed.[39] Further, men and educated people are more likely to be scammed than women and less educated individuals. The type of scam also had an impact on the type of victim. Consumer scam victims were likely to be impulsive, less educated, and older than other scam victims.[40] In contrast, investment scam victims were generally older, educated, and self-controlled males.[41] This indicates that profiling is an established tool used to generate the persona of attacker s and victims of cybercrime.

To further explore attacker personas, we consider a model proposed by Warikoo for an attacker profile specific to cybercrimes. The first step in profiling attackers is to profile the victim. Warikoo proposes a hybrid profiling model with a four-step process for profiling cybercriminals.[42] This includes:

1. profiling the victim including identifying the aspects of the individual or organisation which attracted the cybercriminal. This means the victim's habits must be studied to understand why the victim was chosen by the attacker. This is to understand the criminal mind. In case law, information on whether the offence was intentional and calculated or the victim was randomly chosen is often provided, meaning this step can be satisfied by case law.

2. Identifying the motive behind the cyber-attack. In law, for an individual to be convicted of a criminal offence, the court must be satisfied that there was an *actus reus* and *mens rea*[43]. *Actus reus* means a wrongful act. Thus, it must be established that a criminal act or omission

[36] Robert D. Keppel, Joseph G. Weis, Katherine M. Brown, Kristen Welch, 'The Jack the Ripper murders: a modus operandi and signature analysis of the 1888-1891 Whitechapel murders' (2005) Investigative Psychology and Offender Profiling 2(1) at 15-17.
[37] Duncan Ki-Aries, Shamal Faily and Kristian Beckers, 'Persona-Driven Information Security Awareness' (2016) BISL.
[38] Peter B. Ainsworth, Offender Profiling and Crime Analysis (Routledge 2012) at p7
[39] Monica Therese Whitty, 'Is There a Scam For Everyone? Psychologically Profiling Cyberscam Victims' (2020) European Journal on Criminal Policy and Research 26:399 at p408
[40] Monica Therese Whitty, 'Is There a Scam For Everyone? Psychologically Profiling Cyberscam Victims' (2020) European Journal on Criminal Policy and Research 26:399 at p408
[41] Monica Therese Whitty, 'Is There a Scam For Everyone? Psychologically Profiling Cyberscam Victims' (2020) European Journal on Criminal Policy and Research 26:399 at p407
[42] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 175.
[43] Andrew Cubie, *Scots Criminal Law* (4th edn, Bloomsbury Professional 2016) at 2.1.

was committed[44]. *Mens rea* means a wrongful state of mind and determining whether this is present depends on the crime committed. For example, for murder, the accused must have intended the death or acted with wicked recklessness[45]. Therefore, the intention of the attacker can be established to determine whether *mens rea* is present. This is important as it means that an attacker 's motivation is discussed in case law. Consequently, case law can be used to fulfil this step of Warikoo's process.

3. Empirically analysing the data and identifying trends via statistical analysis. A judge's decision is specific to the case before them, making it case specific. This means that facts and trends about attackers from other cases are not analysed to reach a decision, although the judgements from other cases may be considered. This highlights one weakness of using case law as data and trends among several cases are not identified.

4. Building a profile from the identified characteristics. To build a profile, it must be determined whether the attacker has a pattern. Similarly, in case law, the offender's criminal history[46] is examined and their criminal record is considered. Thus, attacker characteristics can be identified via case law.

Warikoo's proposed methodology composes of 6 profile identification metrics to identify the attacker, as follows.[47]

1. Attack signatures are patterns of identifying information unique to an attacker. For example, "a zero-day attack…implies that a customised code was created" whereas an attack which exposes known vulnerabilities implies that "ready to use tools or known codes" were used.[48] One advantage of case law is that every case is examined in depth. This allows information about the attack to be examined and cases compared to identify the individuality of each case. Thus, any patterns, tools or styles used by the attacker can be identified.

2. Attack methods refers to the method used such as malware, spamming and social engineering.

3. Motivating level relates to the complexity of the attack. Where the attack has a high level of complexity, the attacker has a high motivation level. This indicates they are risk takers and persistent. Warikoo states that when an attacker exploits "multiple layers of vulnerabilities", the attack has a high complexity level whereas an attack which is not continuous is medium level.[49]

[44] Andrew Cubie, *Scots Criminal Law* (4th edn, Bloomsbury Professional 2016) at 2.2
[45] Andrew Cubie, *Scots Criminal Law* (4th edn, Bloomsbury Professional 2016) at 2.18.
[46] Although arguments can be made that examining an offender's criminal history goes against their human right to a fair trial, as having committed a crime in the past does not mean the offender has committed the crime currently on trial: Fiona Raitt, 'The Evidential Use of "Similar Facts" in Scots Criminal Law' (2003) Edinburgh Law Review 7(2)
[47] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174.
[48] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174.
[49] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174.

4. Capability factor refers to the availability of the hacking tools, the attacker's ability to use such tools and the resources used or available to the attacker. This aids in determining the level of capability and the skills and knowledge of the attacker.

5. Attack severity refers to the impact of the attack and the level of disruption caused. In law, any sanctions imposed must be fair and proportionate in the circumstances.[50] Thus, the immediate impact of the offence on that specific victim is considered.

6. Demographics aids in identifying characteristics of the attack as certain types of cybercrimes are common from certain locations. Similarly, jurisdictions, meaning the location of the offence and the court in which the case shall be heard, is considered in law.

It is, however, important to acknowledge the limitations that exist when profiling cyber-crime offenders. One challenge is that often perpetrators of cyber-attacks are remote and may be residing in a different country than the victim, as seen in *McKinnon v Government of the United States of America*[51] and *Love v United States.*[52] Both these cases involve a British citizen committing cybercrimes against US based companies and US Government agencies remotely from their home in the UK. Another challenge in profiling cybercrimes is that an interdisciplinary approach is required. To accurately build a profile of cybercrime offenders, and potentially victims, it is vital to understand law and a technological understanding of cybercrime.[53] However, given that a judge has already applied the understanding of the law on behalf of non-legal experts the use of case law to construct attacker personas would appear to have merit.

3.) The use of Case Law as a Complementary Approach to Building Attacker Personas

This section provides an opportunity for a systematic and critical engagement with case law-based facts[54] or data as a useful complement to building attackers personas. It reviews American legal realism being both a legal theory and a reliable research method for building personas. Meanwhile, to ensure that it is clear why case law is used in this work, it is helpful to understand how the criminal court process works, out of which case law develops. Although the word 'case law' has been defined in the 'definitions' sections above, the process will be laid out below.

A.) American Legal Realism as a Practice -Its System and Procedure:

For a criminal allegation to proceed to court, the initial step is for the alleged crime to be reported to the police and subsequently investigated. If the police believe that sufficient evidence is available to

[50] Scottish Sentencing Council, 'Sentencing Process – Step Eight' (*The Scottish Sentencing Council,* 15 July 2021) <Sentencing process guideline (scottishsentencingcouncil.org.uk)> accessed 27 May 2022.
[51] [2008] 1 W.L.R 1739.
[52] [2018] EWHC 172 (Admin)
[53] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174
[54] See generally Lee Loevinger, "Facts, Evidence and Legal Proof" (1958) 9 Case Western Reserve Law Review 2, 154 Available at Facts, Evidence and Legal Proof (case.edu) accessed 6 August 2022.

support the claim a crime occurred, the police will file a report with the Crown Office and Procurator Fiscal Service.[55] The procurator fiscal's role is to determine whether a crime occurred, whether there is sufficient evidence to prosecute the offence and whether prosecution would be in the public interest, and if so, which court the case shall proceed to.[56] This is a consistent process and each agency involved is impartial and regulated to ensure the correct procedures are followed. This shows consistency and objectivity, suggesting case law is a reliable data source.

Once a case reaches a court, it is the judge's role to decide the outcome of a case. Thus, case law refers to the decision of judges in criminal court cases, as mentioned in the 'definitions' section. These decisions are important as it highlights the ways in which judges interpret and apply legislation or statutes to a specific situation.[57] A judge's decision on whether the accused, the person who allegedly committed the crime, is guilty of the crime and if so, the appropriate sanction, is based on the law and the facts of the case. Thus, decisions are made on a case-by-case basis and "no two cases will ever be exactly the same".[58] Other factors considered are the seriousness of the crime, the background of the accused including any previous recorded crimes committed by the accused, and the harm caused to the victim(s).[59] Thus, case law provides information on the facts of a case, the court's decision and the ratio of the decision, the statute applied (if any), and the sanction imposed, as shall be seen by the cybercrime cases explored later in this work.

B.) American Realism as a Legal Doctrine -Of Theory and Methodology:

A range of information can be gathered via case law including the facts of the case, legal arguments which support and oppose both the victim and the attacker, the damage (if any) caused, the judge's interpretation of the facts and legal arguments, and the decision of the judge(s). Where an attacker is found guilty, the sanction is also detailed. This work argues that the facts of a case can be used to build personas for cybercrimes. There are various strengths and limitations of examining case law to build a persona. To determine whether case law is reliable in theory, the strengths, and limitations of case law, as found in the concept of American Realism, is examined. Thereafter, the information provided by the cases of *McKinnon*, *Love* and *Needham* is compared to Warikoo's identification metrics to determine the reliability of case law in practice.

The most important jurisprudential movement in the twentieth century was American Legal Realism[60]. This had a profound impact on legal reform as those who developed this movement consisted of lawyers, judges, and academics.[61] There were many realists who contributed to the movement, some

[55] SCCJR, 'The Scottish Criminal Justice System' (2019) < https://www.sccjr.ac.uk/wp-content/uploads/2019/10/3-The-Scottish-Criminal-Justice-System.pdf> accessed 17 June 2022.
[56] Justice Committee 9th Report, 2017, 'Role and Purpose of the Crown Office and Procurator Fiscal Service' (SPP 123.1) para5.
[57] Scottish Sentencing Council, 'Introduction to Sentencing' (*The Scottish Sentencing Council*) <Scottish Sentencing Council> accessed 8 June 2022.
[58] Scottish Sentencing Council, 'Introduction to Sentencing' (*The Scottish Sentencing Council*) <Scottish Sentencing Council> accessed 8 June 2022.
[59] Scottish Sentencing Council, 'Introduction to Sentencing' (*The Scottish Sentencing Council*) <Scottish Sentencing Council> accessed 8 June 2022.
[60] Brian Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005) at p50.
[61] Torben Spaak, 'Naturalism in Scandinavian and American Realism: Similarities and Differences' (2009) De Lege, Uppsala-Minnesota Colloquium: Law, Culture and Values 33 at 33.

of which include academics John Chipman Gray (1839-1915) and Karl Llewellyn (1893-1962), and judges Oliver Wendell Holmes (1841-1935) and Jerome Frank (1889-1957).

Realism was a reaction to mechanical jurisprudence, also known as formalism. Formalism argues that judges decide cases based on legal rules and reasons, and this justifies unique decisions in most cases[62]. In response, realists argue the opposite; that court decisions are not based primarily on the law but rather on the judges' idea of what would be fair considering the facts of the case.[63]

The core claim of the American Realism movement is that "judges respond primarily to the stimulus of the facts of the case" and decide based on this initially.[64] Thereafter, judges rationalise their decision with appropriate legal rules and reasons. This has been confirmed by Judge Joseph Hutcheson who stated that "the vital, motivating impulse for the decision is an intuitive sense of what is right or wrong for that cause".[65] Further, Chancellor Kent stated that "he first made himself master of the facts…[and] I then sat down to search the authorities".[66] Thus, decisions are based on nonlegal considerations as legislation and precedent is not considered until after a decision is reached. This highlights the weight of facts as judges rely on established facts when making legal decisions, this implies that such facts can also be relied upon for other purposes, including the creation of attacker and victim personas in the context of cybercrime.

This is supported by Gray's work 'The Nature and Sources of the Law', 1909 in which the importance of case law is emphasised. Gray argues that statutes and precedents are merely sources of law whereas case law and the rules which are formed by judges in cases is the law. This suggests judges in the United States are "truly the lawgiver to all intents and purposes".[67] This shows that case law is reliable and authoritative. As established case facts are the basis for such authoritative decisions, facts are a reliable tool for understanding cybercrimes.

However, while this concept highlights the importance of case law, it results in much scepticism in law. This is because some realists, including Frank, proposed that the law is unpredictable as the law is based on the judge's interpretation of facts and sources of law[68] and judges are humans with needs, limitations, and weaknesses. Consequently, two streams of thought formed. The first is rule sceptics, as supported by Llewellyn, Holmes, and Frank. This focuses on the unpredictability of which rules judges will apply. The other stream consists of fact sceptics who emphasize the uncertainty of facts and, consequently, the limitations of case law as a means of establishing personas for victims and

[62] Brian Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005) at p50.
[63] Brian Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005) at p50.
[64] Brian Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005) at p52. Compare generally with Lee Loevinger, "Facts, Evidence and Legal Proof" (1958) 9 Case Western Reserve Law Review 2, 154 Available at Facts, Evidence and Legal Proof (case.edu) accessed 6 August 2022.
[65] Joseph C. Hutcheson Jr, 'Judgement Intuitive: The Function of the Hunch in Judicial Decision' (1929) 14:2 Cornell Law Review 274 at 285.
[66] Brian Leiter, 'Rethinking Legal Realism: Toward a Naturalized Jurisprudence' (1997) 76 Texas Law Review 267 at 276.
[67] HLA Hart, 'American Jurisprudence Through English Eyes: The Nightmare and the Nobel Dream' (1977) Sibley Lecture Series 33, 11:969 at 975.
[68] Brain Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005) at p54.

attackers. To establish whether case law is reliable, the work of fact sceptic Jerome Frank shall be explored.

In Frank's 'Law and the Modern Mind', 1930, it was argued that judgements may vary with the personality of the judge as a judge's individual bias can influence their decision.[69] This applies to the manner a judge may rationalise their decision as well as their interpretations of the facts of the case. Therefore, neither rules nor facts are fixed or certain, meaning the law is unpredictable. For instance, one judge may be sympathetic towards the facts of a case while another judge may not, thereby influencing their respective decision. This is supported by Holmes who stated that "life of law has been, not logic, but experience".[70] Therefore, as it is possible that bias can influence a judge's decision, case law is not wholly reliable for creating attacker and victim personas. This is because different judges may place an emphasis on different facts of the case, resulting in different judgements and/or sanctions. This impacts personas as, in Frank's opinion, there is not a uniformed and predicable approach to cases.

Frank's argument is valid as it is likely that judges struggle to ignore their "human predispositions when arriving at a legal conclusion".[71] However, this does not mean case law cannot be relied upon. Although depending on the severity of a case, there can be more than one judge deciding on a case. The more serious crimes are tried in Scotland for example by a jury made up of 12 people from the public Thus, the decision reach must be agreed upon by the majority meaning that individual "biases, stereotypes, [and] preconceptions"[72] are balanced and less impactful.

Frank further argued that facts can often be distorted at any stage of collection, presentation, and interpretation. This can influence a judge's interpretation of facts and law. For example, evidence collected by police may be ambiguous or selective in that certain evidence may not be viewed as important to one police officer but may have been vital to the judge making a decision. Therefore, as the judge's interpretation of said facts are the basis for decision made in case law, case law is not wholly reliable. This shows that Frank acknowledges human error which is important as it is an everyday reality. In fact, cybercrimes can often by due to human error as "people remain susceptible to manipulation and thus the human element [of security measures] remains a weak link".[73]

Despite this, Frank's scepticism "sits poorly with practical experience"[74] according to Leiter. While there may be some subjectivity, this is not likely to result in a drastic difference in judgements. Thus, a judge's decision is often predictable as evidenced by solicitors being able to advise their clients of the likely outcome prior to the case going to court. Moreover, in practice, where a party to a court case believes the wrong decision was reached, the decision can be appealed providing certain criteria are met and another set of judges decide whether to uphold the previous decision or overrule the decision. Therefore, there are legal procedures in place to ensure case law is as reliable as possible.

---

[69] [69] Brian Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005) at p54.

[70] Hessel E. Yntema, 'American Legal Realism in Retrospect' (1960) 14(15) Vanderbilt Law Review at p318

[71] Timothy J Capurso, 'How Judges Judge: Theories on Judicial Decision Making' (1998) university of Baltimore Law Review 29:1(2) at p6.

[72] Timothy J Capurso, 'How Judges Judge: Theories on Judicial Decision Making' (1998) university of Baltimore Law Review 29:1(2) at p6.

[73] Francois Mounton, Louise Leenan and H.S Venter, 'Social Engineering Attack Examples, Templates and Scenarios' (2016) Computers & Security at p1.

[74] Brain Leiter, 'American Legal Realism' in Martin P. Golding and William A. Edmundson (eds), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (Blackwell publishing 2005) at p54.

In summary, American legal realism is an important jurisprudential movement as its core concept supports this work. This is because this work proposes that personas can be understood from case law as case facts are reliable, insightful, and impartial. Similarly, realism highlights the importance of established case facts as these facts form the basis of a judge's decision in case law. Thus, in theory, facts provide a sound basis for understanding the characteristics of the attacker and victim.

4.) Some Reflection in Case Law

This section explores the question of whether or how the methodological proposals might be complementary. To determine whether personas can be understood from case law, Warikoo's six identification metrics shall be applied to the following three cybercrime cases. This shall aid in identifying any limitations of case law. Meanwhile, the use of case law in relations to building attacker personas has limits. A short but critical overview of doctrinal research in law therefore precedes the reflection on case law facts.

A.) Approach:

A doctrinal legal research approach, also known as black letter law, is relevant to our work as it is used to evaluate the "meaning and scope of…legal provisions".[75] It is a means to identify the legal rules and the legal principles which legal decisions are based on.[76] To do so, "a critical conceptual analysis of all relevant legislation and case law [is undertaken] to reveal a statement of the law relevant to the matter under investigation"[77]. We examine case law in depth, which differs from socio-legal research examining the laws impact on "society, politics and morality".[78]

As we question the limits of case law, much focus was placed on case law, specifically the cases of *McKinnon v Government of the United States of America,*[79] *Love v United States*[80] and to a lesser extent *Regina v Steffan Needham,*[81] This is important as it is the court's role to interpret facts and statutes and determine how to deal with each case individually, having studied the established facts.[82] By examining the cybercrimes in the above cases and the outcome of the cases, certain behaviours and patterns become apparent in relation to the offender and victim of each case.

[75] Laura Lammasniemi, *Law Dissertation: A Step-By-Step Guide* (Taylor and Francis 2018) at p73
[76] Laura Lammasniemi, *Law Dissertation: A Step-By-Step Guide* (Taylor and Francis 2018) at p66
[77] Terry Hutchinson, 'Valé Bunny Watson? Law Librarians, Law Libraries and Legal Research in the Post-Internet Era', (2014) 106(4) Law Library Journal 579 at 584.
[78] Laura Lammasniemi, *Law Dissertation: A Step-By-Step Guide* (Taylor and Francis 2018) at p74
[79] [2008] 1 W.L.R 1739.
[80] [2018] EWHC 172 (Admin)
[81] [2019] EWCA Crim 1541
[82] See generally Lee Loevinger, "Facts, Evidence and Legal Proof" (1958) 9 Case Western Reserve Law Review 2, 154 Available at Facts, Evidence and Legal Proof (case.edu) accessed 6 August 2022.

The use of offender profiling within law is explained to provide an understanding of offender profiles, with reference to cyber-crimes and personas. The method proposed by Warikoo[83] for constructing offender personas is evaluated, and then applied to three cases to examine whether case law can be used to form personas. The four-step hybrid profiling model is then employed (see the Related Work section) to: recognize the victim's appeal; ascertain the motive behind the attack; spot any relevant trends; and create a profile based on the observed characteristics. Additionally, the proposed six profile identification metrics are used to identify the offender.

The three cases evaluated concern cyber-attacks on a) the state, b) companies and c) individuals. Overall, this aids in determining whether victim profiles can be established via case law. To determine the limits of case law, the theory of American realism is explained as this emphasises the strengths and weaknesses of focusing on the facts of a case.

B.) Sample Cases:

Could Warikoo's six identification metrics support the use of case law to determine or build attacker personas? For a better appreciation of the relevance or relationship between the two approaches, three cases are examined. Each relates to different categories of victimhood, namely 1) the state; 2) the Corporation; and 3) the Individual.

I.) McKinnon vs Government (The State)

McKinnon v Government of the United States of America[84] concerns a Scottish citizen, Gary McKinnon, accessing 97 computers belonging to the United States of America Government from his home computer via the internet between February 2001 and March 2002. This provides information on demographics, under Warikoo's proposed methodology.

Within the case facts, the attack signatures and attack methods used by McKinnon are detailed. Initially, McKinnon identified US Government network computers via an open Microsoft Windows connection. This empowered him to extract identities and passwords of specific administrative accounts. Through the above-mentioned method, he installed remote access and administrative software called 'remotely anywhere'.[85] This is a remote viewing application and is designed for system administration, diagnostics and troubleshooting purposes. Once installed onto a computer, it allows the user to access and control the computer and its files and applications from a remote.[86] Thus, when McKinnon installed this tool on the US Government computer, he was able to access and alter the data on the computers at any time without detection. Once 'remotely anywhere' was installed, McKinnon installed further software tools which enabled him to scan 73,000 US Government computers and moved from network to network. Overall, McKinnon accessed 97 computers which

[83] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174.
[84] [2008] 1 W.L.R 1739.
[85] [2008] 1 W.L.R 1739, para 11.
[86] 'What is RemotelyAnywhere.exe?' (*File.Net*) <RemotelyAnywhere.exe Windows process - What is it? (file.net)> accessed 9 April 2022.

included 53 army computers, 26 navy computers, 16 NASA computers, 1 Department of Defence computer and 1 US Air Force computer.[87]

The attack severity is detailed as the alleged damage caused was widespread. Once McKinnon gained access to the computers, he deleted data from them. This included operating system files which resulted in the US Army's Military District of Washington network of over 2000 computers to shut down for 24 hours. The system became inoperable, and the computers required rebooting. This left the network vulnerable to other cyber-attacks. As well as deleting data, McKinnon copied data and files onto his own computer.[88] Overall, this allegedly resulted in $700,000 worth of recovery work as the "integrity, availability and operation of programmes, systems, information and data" was impaired, rending the computers unreliable.[89]

McKinnon was an unemployed computer systems administrator,[90] suggesting that he had knowledge of computers. Further, he had access to, and the ability to use, hacking tools as evidenced by his attack. Despite this, McKinnon was "tracked down relatively easily, demonstrating his lack of technical savviness".[91] McKinnon stated that this "shows I am not a professional hacker" because professional hackers would not have used their or their partners email addresses to download hacking software.[92] This indicates McKinnon's capability level. He can be termed as script kiddie withy limited skills as he was using open-source hacking tools that are freely available on the Internets.[93]

Information on the motivation level can be inferred from the facts of the case. As analysed, McKinnon not being a professional hacker, he acted alone in his attack targeting the US State. This suggests that hacking into the network was not overly complicated that is supported by the case commentary. McKinnon stated that "he used a very basic tool which scanned for blank passwords and found some very poor security",[94] thus, inferring the lack of a string government network security system.

Based on the information provided by the facts of the case and the case commentary, Warikoo's six identification metrics are answered. The tools and methods employed by McKinnon are disclosed in the sense that it is known he gained access to the computers through weak passwords and an open Microsoft Windows connection. Thereafter, he installed 'remotely anywhere' software, thus, exposing the vulnerabilities in the system, using "ready to use tools or known codes".[95] Therefore, attack signature and attack methods are provided by case law. McKinnon's motivation level is answered.

[87] [2008] 1 W.L.R 1739, para 12.
[88] [2008] 1 W.L.R 1739, para 13 and 14.
[89] [2008] 1 W.L.R 1739, para 15.
[90] [2008] 1 W.L.R 1739, para 4.
[91] Rocci Luppicini (ed.), 'The Changing Scope of Technoethics in Contemporary Society' (2018). Hershey, PA: IGI Global. Compare with Paul Arnell and Alan Reid, 'Hackers beware: the cautionary story of Gary McKinnon'(2009) Information and Communications Technology Law 18:1 at 8
[92] The Independent, 'Gary McKinnon: Inside the Head of a Super Hacker' (*The Independent*, 12 July 2006) < Gary McKinnon: Inside the head of a super hacker | The Independent | The Independent> accessed 2 June 2022.
[93] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174.
[94] Rocci Luppicini (ed.), 'The Changing Scope of Technoethics in Contemporary Society' (2018). Hershey, PA: IGI Global. Compare with Paul Arnell and Alan Reid, 'Hackers beware: the cautionary story of Gary McKinnon'(2009) Information and Communications Technology Law 18:1 at 8.
[95] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174.

McKinnon used "a very basic tool" to gain access to the Government's network.[96] As this is a low level of complexity, his motivation level is the same. However, it is detailed that McKinnon does have knowledge of computer systems and had the tools available which provides information on McKinnon's capability factor. Finally, McKinnon's attack was remote, providing demographics. This shows that an attacker profile can be built from case law as information on all of Warikoo's identification metrics is provided. Information outside of Warikoo's six identification metrics was also provided by case law. This highlights the relevance and reliability of case law.

Primarily, the motivation of the attack is provided by the facts of the case. McKinnon's cyber-attack was "intentional and calculated to influence the United States Government by intimidation and coercion".[97] During an interview, McKinnon stated that his targets were high level US Army, Navy and Air Force computers and his goal was to gain access to the US military classified information network.[98] McKinnon, known in code as SOLO, was a UFO theorist and his motivation for hacking into the US Government's network was to expose the truth about UFOs. McKinnon believed that the government was hiding "alien antigravity devices and advanced energy technologies" which he planned to find and release for humanities sake.[99] In this regard, he wrote the following extract onto one of the compromised US Army computers:

> "US foreign policy is akin to Government-sponsored terrorism these days…It was not a mistake that there was a huge security stand down on September 11 last year…I am SOLO. I will continue to disrupt at the highest level".[100]

As this case concerned extradition, information on McKinnon's health revealed that he suffered from Asperger syndrome, which is a form of autism. He argued that the illness could have caused or triggered the offence. However, not much information on the actual or perceived victim is provided. Therefore, in the context of this paper, the metric that Warikkoo developed is discussed with a focus on offending (and not on victimhood or victims).

II.) Love vs United States (The Private Company)

In *Love v United States,*[101] Love was accused of three indictments for working alongside others in a series of remote cyber-attacks between October 2012 and October 2013. These attacks were on the computer networks of private companies and United States Government agencies including US Army, NASA, US Sentencing Commission, FBI Regional Computer Forensic Laboratory, Deltek Inc, Missile Defence Agency and 6 other agencies.[102]

To do so, Love exploited the known vulnerability of a software application known as Adobe ColdFusion. This provided information on the attack signature and attack method. Adobe ColdFusion is designed to build and administer websites and databases. Through this, he gained unauthorised

[96] Rocci Luppicini (ed.), 'The Changing Scope of Technoethics in Contemporary Society' (2018). Hershey, PA: IGI Global. Compare with Paul Arnell and Alan Reid, 'Hackers beware: the cautionary story of Gary McKinnon'(2009) Information and Communications Technology Law 18:1 at 8.
[97] [2008] 1 W.L.R 1739, para 15.
[98] [2008] 1 W.L.R 1739, para 16.
[99] David Kushner, 'The Autism Defence' (2011) 48(7) IEEE Spectrum 32 at 34
[100] [2008] 1 W.L.R 1739, para 16.
[101] [2018] EWHC 172 (Admin)
[102] [2018] EWHC 172 (Admin), para 5.

access to the computer network. Thereafter, Love carried out 'SQL Injection Attacks' whereby he gained unauthorised access to the databases using manipulated structured query language (A computer program designed to retrieve and manage data of computer databases).

To ensure he could return to the database, Love and others created 'backdoors' within the networks. This enabled Love to exfiltrate confidential information namely telephone numbers, social security numbers, credit card details and salary information. As a result, of the data breach, millions of dollars in damages were paid to the individuals whose data were stolen. Furthermore, dozens of computer servers were substantially impaired.[103] This shows the severity of the attack.

The primary focus of this case was the extradition of Love to America, which led to the provision of information about Love as the attacker. Love is a British national, with mental and physical health conditions. Love suffers from Asperger Syndrome which was considered "a very severe disability" as it results in Love becoming absorbed in his interests so much that he neglects other aspects of his life including his studies and health[104]. Due to this, Love was described as a "sophisticated and prolific computer hacker who specialised in gaining access to the computer networks of large organisations".[105] This shows Love's motivation level and capability factor.

Like *McKinnon*, *Love* provides all necessary information for the 6-point identification metrics proposed by Warikoo to build an offender profile. Love gained access via vulnerabilities in Adobe ColdFusion and carried out 'SQL Injection Attacks' thus revealing the attack signature and method. Love has knowledge of computer and security systems and has experience in hacking. Thus, Love's capability is detailed. Further, Love was accompanied by other hackers, suggesting a medium level of complexity. This suggests Love has a medium to high motivation level which is likely linked to his disability. The severity of the attack is demonstrated by the fact that there were several victims to this attack; private companies, government departments and the individuals whose personal details were stolen. Finally, information on demographics is provided as Love was remotely located.

However, again, very little information is provided on the victims.[106] It is known that Adobe ColdFusion was used to gain access meaning this must have been a common feature on the private company's computers and the government computers.

III. Regina vs Steffan Needham (The individual)

Another case which involved a company was *Regina v Steffan Needham*[107] in which an ex-employee used another employee's login credentials to access the employer's system and deleted 23 servers as revenge for his termination of employment. The accused experienced depression, anxiety, and a paranoid personality disorder, leading to the conclusion that they were impacted to a greater extent

[103] Gemma Davies, 'Extradition, Forum Bar and Concurrent Jurisdiction: Is the Case of Love a precedent for Trying Hackers in the UK? Lauri Love v (1) The Government of the United States of America (2) Liberty' (2018) 82(4) J. Crim. L 296 at 296
[104] [2018] EWHC 172 (Admin), para 75.
[105] Gemma Davies, 'Extradition, Forum Bar and Concurrent Jurisdiction: Is the Case of Love a precedent for Trying Hackers in the UK? Lauri Love v (1) The Government of the United States of America (2) Liberty' (2018) 82(4) J. Crim. L 296 at 296
[106] [2018] EWHC 172 (Admin), para 17.
[107] [2019] EWCA Crim 1541

than the average person would be.[108] However, the attack was premeditated, and the actions of the accused led to substantial damage to the business, financial losses, and harm to customers. Additionally, the employee whose credentials were exploited by the accused to gain access was subsequently terminated.[109]

This is a different situation from *Love*. In *Love,* the offender used remote access to hack into the network via vulnerabilities in the software application. In *Needham*, the offender used authorised access, albeit not his own authorised access. The employer mistakenly believed that the accused's credentials had been deleted from the system.[110] Thus, *Love* concerns hacking into a company's network; and *Needham* concerns unauthorised access using credentials provided by the company. This is important as it shows that there are various methods of cyberattacks and that Warikoo's metrics can be applied to different types of attacks.

Through the facts presented in *Regina v Steffan Needham*, information regarding the attack signature and method is disclosed. In this case, access was obtained using credentials provided by the company. This also highlights that the offender was not a highly skilled hacker as there were no hacking tools used or available to the attacker. Further, as in the other two cases, the attack was not complex. Nevertheless, significant damage was inflicted upon the business, underscoring the severity of the attack. Although the attack originated from the offender's home, both the perpetrator and victim were in the UK, providing insights into the geographical demographics involved.

5.) Building Attacker Personas: An Analytical Summary

In relation to whether case law in practice is reliable for understanding personas, it is necessary to reflect on the information provided in *McKinnon*, *Love and Needham* and the extent to which the facts of the cases correlate with Warikoo's identification metrics.

In each case, all six of Warikoo's identification metrics can be recognized via the facts of a case, some metrics more than others. This is because, depending on the type of victim, certain information may not be disclosed in case law. Where the victim is the state, as seen in both *McKinnon*[111] and *Love,*[112] certain information may be confidential. The severity of the attack, for example, although mentioned in all three cases, was ambiguous and it is not determined whether the alleged damage is an accurate representation of the harm caused. In fact, in *McKinnon,*[113] McKinnon denied that he caused any damage at all, yet the state argued that the alleged damage was $700,000 worth.[114] Despite this, sufficient information was provided to answer all of Warikoo's metrics. Moreover, information beyond these six metrics is provided in each case. This suggests that relying on case law may enable a more accurate and insightful persona to be created.

[108] [2019] EWCA Crim 1541, para 31.
[109] [2019] EWCA Crim 1541, para 11 and 14.
[110] [2019] EWCA Crim 1541, para 5.
[111] [2008] 1 W.L.R 1739.
[112] [2018] EWHC 172 (Admin).
[113] [2008] 1 W.L.R 1739.
[114] [2008] 1 W.L.R 1739, para 15.

Primarily, case law facts may reveal and address the physical and mental health of the accused when it is appropriate and relevant to the case.[115] In the case of McKinnon, evidence was presented indicating that he suffered from Asperger syndrome, which is a form of autism. One trait of Asperger syndrome is that many people have "intense and highly focused interests". McKinnon had a fixation for computers and space, particularly the idea that alien life and UFOs exist.[116] This motivated him to hack into the US Government network. McKinnon told the Guardian, "You end up lusting after more and more complex security measures…It was addictive. Hugely Addictive"[117] and "a very unhealthy obsession".[118]

Similarly, Love also suffered from Asperger syndrome which was described by Professor Baron-Cohen as a "very severe disability".[119] This is because it causes obsessive traits, with Love being so consumed in his interests that he would neglect his health and studies.[120] Further, due to the Asperger's syndrome, Love had "no regard for the consequences of his actions".[121]

This is important as there are certain character traits or "classic patters of Asperger's".[122] Those with Asperger syndrome are often highly intelligent people who have an IQ in the average range or above.[123] They are likely to have a narrow attention span and obsess over their interests, with more than 50% of people with Asperger's having an obsessive interest in technology, physics, and space.[124] It has been found those with Asperger's often lack understanding of social cues and the impact their obsessive behaviour may have.[125] While this does not mean that everyone with Asperger syndrome will be obsessive and may commit a crime which relates to that obsession, it does suggest that this disability may be a common trait of cybercriminals. This is supported by Paul who states that "there have been an inordinate number of young men with Asperger's who have gotten in trouble with the law".[126] This shows that case law is reliable as the health of McKinnon and Love was revealed in each case. Thus, using case law enables a broader and more accurate profile of the attacker to be understood as personality and characteristics of the accused can be developed.

Another advantage of relying on case law to understand personas is that information on the motive is provided. Warikoo provides a four-step process for profiling cybercriminals and the second step is to identify the motive behind the cyber-attack. This is important because "a motive is closely associated with a victim". Therefore, by comprehending the motive, one can gain insight into why a particular victim was targeted, allowing for an understanding of victim behaviour and characteristics. This aids

[115] See generally Lee Loevinger, "Facts, Evidence and Legal Proof" (1958) 9 Case Western Reserve Law Review 2, 154 Available at Facts, Evidence and Legal Proof (case.edu) accessed 6 August 2022.
[116] David Kushner, 'The Autism Defence' (2011) 48(7) IEEE Spectrum 32 at 36.
[117] Jon Ronson, 'Game Over' The Guardian (2005) <Game over | Gary McKinnon | The Guardian> accessed 14 June 2022.
[118] The Independent, 'Gary McKinnon: Inside the Head of a Super Hacker' (*The Independent*, 12 July 2006) < Gary McKinnon: Inside the head of a super hacker | The Independent | The Independent> accessed 2 June 2022.
[119] [2018] EWHC 172 (Admin), para 75.
[120] [2018] EWHC 172 (Admin), para 75.
[121] [2018] EWHC 172 (Admin), para 62.
[122] David Kushner, 'The Autism Defence' (2011) 48(7) IEEE Spectrum 32 at 37.
[123] Simon Baron-Cohen, 'The Cognitive Neuroscience of Autism' (2004) 75(7) Journal of Neurology, Neurosurgery and Psychiatry 945 at 945.
[124] David Kushner, 'The Autism Defence' (2011) 48(7) IEEE Spectrum 32 at 37.
[125] David Kushner, 'The Autism Defence' (2011) 48(7) IEEE Spectrum 32 at 34.
[126] David Kushner, 'The Autism Defence' (2011) 48(7) IEEE Spectrum 32 at 34.

in building attacker and victim personas as the motives were mentioned in the case of McKinnon.[127] *Love*[128] and *Needham.*[129]

In *Needham,*[130] the motive was revenge for his employer terminating his employment after the probation period. Interestingly, this was linked to the accused's medical history. Needham suffered from depression, anxiety, and a paranoid personality disorder, which caused "low self-esteem and feelings of inadequacy".[131] Due to losing his job, Needham experienced a sense of humiliation. Given his sensitivity to humiliation, he was more susceptible to a heightened reaction compared to others.[132] Consequently, Needham planned a cyber-attack. Prior to losing his job, on the 17th May, Needham checked the policies for himself and a colleague with the username Speedy. This was because he had been aware there was a likelihood his employment would be terminated. On the 18th May, Needham carried out the cyber-attack.[133] Thus, this was a calculated and motivated attack which he knew was wrong as he used his colleagues' credentials to not be caught.

6.) Conclusions

A persona identifies "relevant behaviours and perceptions" of users of data.[134] Thus, by building an attacker persona, the behaviour of the attacker can be understood, characteristics can be identified and information on the cyber-attack can be gathered and analysed. A proposed method for profiling cybercriminals is via Warikoo's identification metrics. This requires information to be gathered on the attacker's attack signature, attack method, motivating level, capability factor, attack severity and demographics.[135] But, whilst profiling attackers is not a novel concept, understanding profiles via case law is. Thus, this work offers a different and interdisciplinary outlook on attacker personas for cybercrimes. The limitations and strengths of relying on case law were analysed in theory via American realism to determine its reliability to understand persona, and in practice, via the cases of *McKinnon*, *Love* and *Needham.* Thus, it was found that case law is suitable and reliable.

On a critical note, compilation and interpretation of case law facts do possess a degree of subjectivity. This is to be expected since judges are human and susceptible to errors and weaknesses. However, Frank's assertion that a judge's bias would significantly impact a judgment to the point of rendering it unpredictable is somewhat limited. This is because, in the modern Scottish court system, there are procedures and safeguards to ensure that judgements are fair and proportionate.[136] For example, legislation may provide the sentence that should be imposed if found the accused is found guilty. This

[127] [2008] 1 W.L.R 1739.
[128] [2018] EWHC 172 (Admin)
[129] [2019] EWCA Crim 1541
[130] [2019] EWCA Crim 1541
[131] [2019] EWCA Crim 1541, para 13.
[132] [2019] EWCA Crim 1541, para 13.
[133] [2019] EWCA Crim 1541, para 7 and 8.
[134] Duncan Ki-Aries, Shamal Faily and Kristian Beckers, 'Persona-Driven Information Security Awareness' (2016) BISL.
[135] Arun Warikoo, 'Proposed Methodology for Cyber Criminal Profiling' (2014) Information Security Journal: A Global Perspective 23:172 at 174.
[136] Scottish Sentencing Council, 'Sentencing Process – Step Eight' (*The Scottish Sentencing Council,* 15 July 2021) < Sentencing process guideline (scottishsentencingcouncil.org.uk)

limits the argument that a sympathetic judge may impose a harsher sanction. Where a legal error has been made, parties have the right to appeal the judgement. If accepted, the case would go to the appeal court in which three or five judges are likely to decide whether the decision should be upheld or rejected.[137] This ensures that a conviction and/or sentence abides by the law and that a judge has not erred in the decision. Other measures to ensure impartiality is for more than one judge to make the decision or for a jury of many more people to reach a verdict after hearing the facts and instructions given by the judge.[138] Therefore, while there is room for human error, measures exist to ensure fairness, objectivity and integrity of case law facts.

Moreover, one significant advantage is that case law delves deep into the circumstances of a cyberattack and includes information on the attacker and their background. Therefore, case law can offer further insight into an attacker persona than Warikoo's six identification metrics, suggesting case law is a reliable tool to build attacker personas. As seen via *McKinnon,*[139] *Love*[140] and *Needham,*[141] information on the attackers' health is provided, where relevant to do so, as well as the attackers' motive for the attack. While in the cited cases, there was a connection between health and motive, this correlation may not always exist, and therefore, the health of the accused may not be disclosed in such circumstances. However, the health of the attacker can offer valuable insights into their characteristics or traits, such as intelligence, drive, social unawareness, sensitivity to humiliation, and more, as demonstrated in the cited cases.

Case law facts, in turn, contribute to a more comprehensive understanding of an attacker persona. Despite its limitations, the advantages of the insights it provides outweigh these limitations. The use case law, rather than merely complementing existing models, could develop further and offer a better alternative to software designers seeking to build attacker personas. Future work could involve a broader analysis of the types of cybercrime cases identified in case law to determine different types of attacker personas. Additionally, further research into the reliability of using case law facts to understand personas could be conducted, such as determining the accuracy of using Warikoo's six identification metrics to profile cybercriminals.

[137] Scottish Courts and Tribunals, 'Criminal Appeals' (*Scottish Courts and Tribunals)* < Criminal Appeals (scotcourts.gov.uk)> accessed 14 Junes 2022.
[138] Scottish Courts and Tribunals, 'Participating in Jury Trails in Scotland' (*Scottish Courts and Tribunals*, 23 May 2022) <Jurors (scotcourts.gov.uk)> accessed 14 June 2022.
[139] [2008] 1 W.L.R 1739.
[140] [2018] EWHC 172 (Admin)
[141] [2019] EWCA Crim 1541