CLAIRE REES

THE LEGITIMACY OF THE USE OF OPEN-SOURCE INFORMATION BY NEW ZEALAND'S INTELLIGENCE AGENCIES

Submitted for the LLB (Honours) Degree 2022

Faculty of Law

Victoria University of Wellington

2022

Abstract:

This paper analyses the legitimacy of the use of publicly available information by New Zealand's intelligence and security agencies, as authorised by the Intelligence and Security Act 2017. The Act establishes a legislative framework, requiring agencies to obtain a warrant before undertaking "unlawful" activities. Under the Act, agencies' collection, obtaining and use of publicly available information is considered a "lawful" activity, meaning agencies are not required to obtain a warrant. However, given the practical reality of the nature and volume of public information available to agencies following technological advancements, this position fails to sufficiently protect individual's human rights. This paper focuses on two main human rights. Firstly, the paper argues that agencies' ability to aggregate publicly available information to form revealing images of individual's crosses the boundary from public information to private information, thereby breaching reasonable expectations of privacy. Secondly, the paper argues that the collection of publicly available information by agencies could potentially be considered an "unreasonable search or seizure" under s 21 of the NZBORA, by analysing domestic and international approaches taken to novel surveillance technology. Ultimately, this paper concludes that the Act is unfit to sufficiently protect individual's human rights in the face of modern technology, thus requiring urgent legislative and political attention.

Key words: "Publicly Available Information"**,** "Intelligence and Security Act 2017", "Privacy", "Security", "Unreasonable Search or Seizure".

Table of Contents:

I Introduction:

With the evolution of the internet, the distinction between the public and the private realm has blurred markedly. Websites such as Facebook, Instagram and LinkedIn see us share exponential volumes of our lives, posting photos and life updates to create digital biographies of ourselves. While users have actively consented to each piece of information being shared with the world at large, individuals are unlikely to be aware that this information can later be combined by intelligence agencies, forming a revealing and deeply sophisticated image of us. The question thus arises, at what point does the Government's collection cross the boundary from public to private information?

The issue arises in the Intelligence and Security Act 2017. The Act consolidates the objectives, functions and powers of New Zealand's two intelligence agencies, the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB), in a single statute.[1] The aim of the Act is to provide clarity to the public about what activities agencies are authorised to carry out to assist in their function of identifying threats to New Zealand's national security and economic well-being.[2] Under the Act, intelligence agencies are permitted to collect, obtain and use publicly available information about citizens without requiring a warrant.[3] In contrast, agencies are not permitted to conduct mass surveillance, including active monitoring of the internet, or conduct a "search" of places, people or things, without first obtaining authorisation from the authorising Minister and the Chief Commissioner of Intelligence Warrants.[4] The rationale underpinning this distinction is that by placing information in the public domain, individuals have relinquished any right to a reasonable expectation of privacy in respect of the information.[5] However, while this position follows traditional notions of privacy, it fails to account for privacy interests that arise from information being aggregated in a way that reveals more about an individual than intended.

This paper evaluates the legitimacy of the use of publicly available information by New Zealand's intelligence agencies through a human-rights lens, focusing on whether the

[1] Michael Cullen and Patsy Reddy *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (New Zealand Parliament, 29 February 2016) at [14].
[2] At [25] – [26]; Intelligence and Security Act 2017, s 3.
[3] Christopher Finlayson *Obtaining and using publicly available information* (New Zealand Intelligence Community, Ministerial Policy Statement, September 2017) at [2].
[4] Intelligence and Security Act 2017, s 67.
[5] Finlayson, above n 3, at [5].

potential infringement of a person's individual rights is appropriate in the pursuit of collective security. To begin, section II describes New Zealand's security context. Next, section III outlines the importance of Open-Source Intelligence. Section IV describes the Act's current legislative framework authorising agencies' use of publicly available information. Section V argues the Act's current position is not in line with human rights standards as it focuses on the lawfulness of the collection of a single piece of publicly available information. In doing so, it fails to take into account that the aggregation of information may breach two fundamental individual human rights; the right to privacy, and the right to be secure against unreasonable search and seizure. Section VI frames the nature of the privacy issue by giving the example of Clearview, a private security company, that scrapes individuals' public information from the internet and creates a database capable of identifying people from their uploaded photos. Section VII analyses whether agencies' ability to piece together a picture of a person's life and activities using publicly available information could be considered a search, thereby breaching s 21 of the NZBORA. The section also considers international approaches to technological advancements, including the mosaic theory developed by Courts in the United States in response to large scale data collection by public sector agencies. Ultimately, this paper concludes that given the potential erosion of an individual's rights, greater protections are required before agencies can access all publicly available information. Accordingly, the Act requires both legislative and political attention. Section VIII considers two potential approaches that could be taken to establish certainty in an increasingly contested area.

II New Zealand's Security Context:

Throughout this paper, the approach is taken that the use of publicly available information by intelligence agencies is not legitimate if it significantly erodes individuals' rights. However, in some instances, such breaches may be justified in the collective interest of national security. Where the balance falls will depend upon whether the reality of a security risk within a nation is proportionate to any potential limitations on an individual's rights and freedoms.[6] For instance, in times of high-risk security threats, the security of the state will often be the prime consideration.[7] In contrast, when a security risk is deemed low, individual freedom and autonomy are considered fundamental and any security activity is deemed to

[6] David Omand, Jamie Bartlett and Carl Miller "Introducing Social Media Intelligence (SOCMINT)" (2012) 27(6) Intell Natl Secur 801 at 816.
[7] Cullen and Reddy, above n 1, at *Foreword.*

threaten these rights.[8] This paper will not focus on New Zealand's current threat landscape. However, it is necessary to briefly provide context of the New Zealand public's changing opinion towards national security.

New Zealand is a liberal democratic state meaning intelligence and security agencies face significant restraints on their use of security apparatus.[9] When carrying out activities, agencies face the same constraints that other governmental departments do. This means that agencies have neither the financial capability, legal authority nor social licence to conduct mass surveillance on the public.[10] Prior to the 15th March 2019 when New Zealand's Muslim community suffered a terrorist attack killing 51 citizens, studies suggested some of the New Zealand public appeared to feel the nation had a low threat of terrorism.[11] In October 2014, a Security Issues Poll of 1,000 adults found 48% of respondents believed New Zealand faced no or minimal risk from security threats.[12] Additionally, domestic controversies had significantly undermined public confidence in how intelligence agencies comply with the law and privacy concerns.[13] For example, in 2012, it emerged that Kim Dotcom, a high profile German entrepreneur, had been subject to unlawful surveillance by the GCSB, involving the interception of his private communication as a New Zealand permanent resident.[14] A subsequent review of the GCSB's legal compliance identified that at least 88 people had been subject to unlawful surveillance.[15] Accordingly, in 2014, a survey carried out by the Privacy Commissioner found 52% of respondents were actively concerned about surveillance by NZ's intelligence agencies.[16] Thus, the politico-legal context was reflected at the time of the drafting of the Act in 2017.[17] The Act is designed as a robust legislative framework to ensure that agencies are able to carry out their operational work lawfully, without compromising any of the freedoms New Zealanders exercise.[18]

---

[8] At *Foreword.*
[9] Andrew Little, Minister of Health of New Zealand "Intelligence and Security in Our Changing World" (Speech to the Victoria University of Wellington Centre for Strategic Studies, Wellington, 4 November 2021).
[10] Little, above n 9.
[11] Cullen and Reddy, above n 1, at [1.2].
[12] At [1.12].
[13] Damien Rogers "Intelligence and Security Act 2017: A Preliminary Critique" (2018) 4 NZ L Rev 657 at 665.
[14] At 665.
[15] At 662.
[16] Cullen and Reddy, above n 1, at [1.11].
[17] Rogers, above n 13, at 659.
[18] Little, above n 9.

However, public attitudes towards privacy and security are not fixed and will change over time, particularly in response to events such as terrorist attacks.[19] Therefore, it is important that security legislation is regularly reviewed. Following the Christchurch massacre, the Prime Minister appointed two independent reviewers, Sir Terence Arnold KNZM and Matanuku Mahuika, to undertake a periodic statutory review of the Intelligence and Security Act 2017, due to be presented to the parliamentary Intelligence and Security Committee by 20th December 2022.[20] The review aims to determine whether improvements can be made to the Act to ensure it continues to be "effective, clear and fit for purpose".[21] Similar to the issues being considered in this paper, the review will have particular regard as to whether the Act appropriately balances national, community and individual security with individual privacy and other rights,[22] whether the authorisation framework can be improved to better serve the purpose of the Act,[23] and whether the Act provides appropriate protections and oversight for the collection of intelligence.[24]

The independent reviewers have placed significant emphasis on engaging with the public to hear their opinions on the Act, particularly in whether it strikes the right balance between security and rights and freedoms.[25] Rebecca Kitteridge, director of the NZSIS, has also stressed the importance of public discussion about national security, particularly surrounding the trade-off between technology and privacy, noting "…it is interesting to see how the narrative goes, we don't want intelligence agencies to conduct mass surveillance to why weren't the intelligence agencies conducting mass surveillance".[26] Similarly, Andrew Little, Minister for the GCSB and the NZSIS has said that the public needs to be consulted about whether they want spies "trawling through their Trade me and Facebook accounts".[27]

[19] Cullen and Reddy, above n 1, at [1.15].
[20] Ministry of Justice "Review of the Intelligence and Security Act 2017: Progress Report No 1" (1 August 2022) <www.justice.govt.nz >.
[21] Ministry of Justice "Review of the Intelligence and Security Act 2017: Terms of Reference" (1 August 2022) <www.justice.govt.nz> at [1.1].
[22] At [2.1].
[23] At [2.3].
[24] At [2.4].
[25] Ministry of Justice "Intelligence and Security Act Review" (2 September 2022) < www.justice.govt.nz>.
[26] Thomas Manch "More data surveillance and less privacy? Spy chief says the public must decide" *Stuff* (online ed, New Zealand, 12 June 2021).
[27] Manch, above n 26.

III Importance of Open-Source Intelligence:

Open-Source Intelligence (OSINT) is the intelligence output from the systematic collection and material processing of open-source information (OSINF).[28] OSINF includes all publicly accessible information, found either online or offline, across a range of mediums.[29] Despite emphasis often being placed on "secret intelligence", across the world, the majority of intelligence collection involves utilising open-sources. In 2012 in New Zealand, it was estimated that approximately 90 to 95% of intelligence reports use open source information.[30] Further, the former United States Director of Central Intelligence, Allen Dulles, believes that a proper analysis of OSINT would supply the United States with over 80% of the information that is required to guide national policy.[31] Similarly, the British, Swedish and Dutch Ministries of Defence and Intelligence Agencies use OSINT for at least 90% of their intelligence collection.[32]

The main reason for OSINT's worldwide popularity is that it is deemed to be the only fully legal intelligence collection method by focusing on the collection of information that has already been published publicly. [33] Generally, this type of information involves that which the creator was not concerned to keep secret.[34] Therefore, OSINT is deemed to be non-intrusive, less risky and to not violate human rights.[35] Further, with the growth of social media and digital interconnectedness, the volume of information that is able to be collected online significantly outweighs other methods, including those available through secret sources.[36]

The use of publicly available information underpins the activities carried out by both the NZSIS and GCSB. NZSIS is New Zealand's human intelligence agency, focusing on obtaining intelligence from people with knowledge or access to information across a range of

[28] Nihad Hassan and Rami Hijazi "Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence" (Apress Berkeley, California, 2018) at 4.
[29] At 5.
[30] Cullen and Reddy, above n 1, at 32.
[31] Hamid Akin Ünver *Digital Open Source Intelligence and International Security: A Primer* (EDAM Research Reports, Cyber Governance and Digital Democracy, July 15 2018) at 5.
[32] At 5.
[33] Gašper Hribar, Iztok Podbregar and Teodora Ivanuša "OSINT: A "Grey Zone"?" (2014) 27(3) Int J Intell CounterIntell 529 at 530.
[34] Royal Commission of Inquiry into Terrorist Attack on Christchurch Mosque "Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019" (2020) at 533.
[35] Hribar, Podbregar and Ivanuša, above n 33, at 530.
[36] Cullen and Reddy, above n 1, at 32.

collection methods, including open-source research.[37] For example, the NZSIS may use information collected from publicly accessible forums to produce intelligence reports about threats of terrorism or violent extremism.[38] GCSB is New Zealand's signals intelligence agency, focused on identifying, collecting and reporting on target communications.[39] Therefore, the GCSB may utilise publicly available technical information to research and develop methods of obtaining information.[40] The importance of OSINT, particularly online, was made evident on 15th March 2019 during the Mosque terrorist attack. It was on the internet that the individual developed and disseminated his extreme right-wing views, researched different firearms, and obtained operational guidance.[41] The report that followed the attack concluded that a significant portion of New Zealand's counter-terrorism efforts in the future needs to be done online as the internet is increasingly being used as a "key platform for terrorist radicalisation and recruitment".[42]

IV Publicly Available Information: The Legal Framework:

A Authorisation Framework:

The Intelligence and Security Act 2017 establishes an authorisation framework that determines what activities agencies are lawfully empowered to carry out without requiring an authorisation, and in what instances they must apply for a warrant.

As per s 48, an agency may carry out a lawful activity in the performance or exercise of any function, duty or power, without requiring authorisation.[43] However, as per s 49(1), an agency must seek authorisation via a warrant to carry out any activity that would otherwise be unlawful, except in a situation of urgency.[44] Importantly, s 49 complements s 17 which imposes an overarching constraint on the agencies to act in accordance with New Zealand law and all human rights obligations.[45]

---

[37] New Zealand Intelligence Community "New Zealand Security Intelligence Service (NZSIS)" <www.nzic.govt.nz>.
[38] Finlayson, above n 3, at [13].
[39] Government Communications Security Bureau "Intelligence Collection" <www.gcsb.govt.nz/>.
[40] Finlayson, above n 3, at [13].
[41] Royal Commission of Inquiry into Terrorist Attack on Christchurch Mosque, above n 34, at 533.
[42] At 408.
[43] Intelligence and Security Act 2017, s 48.
[44] Section 49.
[45] Section 17.

Under the Act, the collection, obtaining and use of publicly available information by intelligence agencies is considered a "lawful activity".[46] This means that agencies are not required to obtain a warrant. However, agencies are required to exercise care to ensure that only public information is collected, otherwise a warrant or other authorisation is required.[47]

B Definition of Publicly Available Information:

Under the Act, *publicly available information* is defined as information that:[48]

(a) Is published in printed or electronic form or broadcast:

(b) Is generally available to members of the public free of charge or on payment of a fee:

(c) Is included in a public register (including public registers not covered by the Privacy Act 1993).

This definition includes information that has been posted online by individuals with an unrestricted audience, so that any member of the public would be able to retrieve and view the information from their computer at any time.[49] For example, an image posted on a public setting such as Instagram would be included. In these instances, it is assumed that the individual has relinquished their right to any reasonable expectation of privacy they may have regarding the use of that information.[50] However, this definition also includes other published public information such as sports results, school newsletters, photos taken at public events or information in public registers such as electoral rolls, motor vehicle licences or birth and death registers.

In contrast, information is not considered publicly available where it is shared within a closed group and an additional step is necessary before any member of the public can view it.[51] For example, photos posted to a private Instagram account will not be considered available as the sharer must approve new followers before the information can be accessed.[52] In these instances, the sharer would be assumed to have a reasonable expectation that the information would remain private within the group.[53]

---

[46] Finlayson, above n 3, at 1.
[47] At [31].
[48] At 1.
[49] At [5].
[50] At [5].
[51] At [6].
[52] At [6].
[53] At [6].

C Collection of Publicly Available Information:

1 Collection Methods:

Under the Act, the GCSB and NZSIS are empowered to collect publicly available information using collection methods not available to the public.[54] This could involve using specialist intelligence techniques, or through relationships with people who have access to the information such as human sources. In using methods not available to the public, the agencies must take care to ensure that it does not involve any unlawful activity, unless done so with an authorisation under Part 4.[55] Therefore, while the Act authorises agencies to legally collect publicly available information without a warrant, their collection method must not involve an unlawful activity.

The Act does not clearly establish the scope of what is "unlawful".[56] The Act defines unlawful activities to include the commission of criminal offences under the Crimes Act 1961 and otherwise, and behaviour that is contrary to statute, such as the Privacy Act 2020 and the New Zealand Bill of Rights Act 1990.[57] Therefore, if the collection method involves an offence, such as breaching the Privacy Act, an agency is required to obtain a warrant. However, it is unclear under the Act whether "unlawful" encompasses civil wrongs, such as trespass, a breach of contract or the tort of privacy.[58] The tort of privacy, established in New Zealand by the Court of Appeal in *Hosking v Runting,* protects unreasonable interference with an individual's privacy.[59] There are two requirements to establish a successful claim; an existence of facts of which there is a reasonable expectation of privacy, and publicity given to those facts that would be considered highly offensive to an objective reasonable person.[60]

The lack of definition of "unlawful" becomes a significant issue where agencies appear to breach a civil wrong, such as the tort of privacy, as it is unclear whether they must obtain a warrant. For example, information can be hacked by a company from a private database and placed publicly online. In this instance, the tort of privacy has been breached as claimants have a reasonable expectation of privacy in respect of the information, and the information

[54] At [32].
[55] Finlayson*,* above n 3, at [32].
[56] Royal Commission of Inquiry into Terrorist Attack on Christchurch Mosque, above n 34, at 568.
[57] At 568.
[58] At 568.
[59] *Hosking v Runting* [2005] 1 NZLR (CA) at [117].
[60] At [117].

has been publicised to the world at large which would be considered highly offensive. However, as the information has entered the public domain, it falls under the Act's definition of "publicly available information". Usually, an intelligence agency would not require an authorisation to obtain such material. However, as the information has been released illicitly, arguably, the subsequent acquisition by an agency should be considered an "unlawful" collection method, thereby requiring a warrant.

2 Lack of consent required during collection:

The Privacy Act 2020 is a legislative regime that protects individual's privacy by setting out 13 information privacy principles for how businesses, organisations and public sector agencies should collect, process and retain personal information.[61] While the principles act as clear guidance, they do not confer on any person any legal right meaning there is no remedy available for a claimant where a breach occurs.[62] Under Principles 2, 3 and 4 of the Privacy Act, organisations are required to collect personal information directly from the individual concerned unless publicly available,[63] take reasonable steps to ensure the individual is aware the information is being collected,[64] and collect in a way that is lawful and "fair and reasonable in the circumstances".[65] The NZSIS and GCSB are subject to most information privacy principles.[66] However, due to their statutory functions requiring the maintaining of secrecy, the GCSB and NZSIS are exempted from principles 2, 3 and 4(b) of the Privacy Act.[67] This means agencies do not have to collect personal information directly from the individual concerned, or take reasonable steps to ensure the individual is aware or consents to their information being collected.

D Authorisation of Warrants:

Where an activity is deemed unlawful, Part 4 of the Act establishes certain criteria that must be satisfied before a warrant is issued. The agency must make a case to the authorising

---

[61] Nessa Lynch and others *Facial Recognition Technology in New Zealand Towards a Legal and Ethical Framework* (Law Foundation New Zealand, Wellington, 2020) at [2:7].
[62] Privacy Act 2020, s 31.
[63] Privacy Commissioner "Principle 2: Source of personal information – collect it from the individual" <www.privacy.org.nz>.
[64] Privacy Commissioner "Principle 3: Collection of information from subject – what to tell the individual" <www.privacy.org.nz>.
[65] Privacy Commissioner "Principle 4: Manner of collection <www.privacy.org.nz>.
[66] Andrew Little *Collecting Human Intelligence* (New Zealand Intelligence Community, Ministerial Policy Statement, 1 March 2022) at [50].
[67] Privacy Act 2020, s 28; Privacy Commissioner "Intelligence and Security Act amendments to Privacy Act: FAQs" <www.privacy.org.nz>.

Minister and the Chief Commissioner of Intelligence Warrants that the activity is "necessary and proportionate" given the intelligence outcome being sought.[68] This requires specific details of the operational activity, and illustrating that the purpose of the warrant cannot be achieved by less intrusive means.[69]

Following the granting of a warrant, agencies are given powers under the Act to give effect to an otherwise unlawful activity. Amongst other activities, this includes:[70]

(a) conducting surveillance in respect of 1 or more –
    (i) persons or classes of persons:
    (ii) places or classes of places:
    (iii) things or classes of things:
(b) searching 1 or more –
    (i) places or classes of places:
    (ii) things or classes of things:

V Does the Act's current position appropriately balance human rights standards?

> In the technology mediated world, privacy law and society are in a state of confusion about the appropriate treatment of publicly available personal information.[71]

Prima facie, the Act's position in authorising the use and collection of publicly available information appears to appropriately balance human rights standards. As people have moved to transferring more of their lives online with the evolution of the internet, digital platforms have become increasingly essential sources of information in the context of security and public safety.[72] However, while digital spaces are public, the subsequent gaining and access to information by government authorities on these platforms is increasingly being criticised, being suggested to be akin to surveillance.[73] This section will use a human rights framework as an analytical tool to consider whether the potential erosion of individuals rights is legitimate.

---

[68] Intelligence and Security Act 2017, s 61 (a).
[69] Section 61 (c).
[70] Section 67 (1).
[71] Joel Reindeberg "Privacy in Public" (2014) 69 Mia L Rev 141 at 141.
[72] Kira Vrist Rønn and Sillie Obelitz Søe "Is Social Media Intelligence private? Privacy in public and the nature of social media intelligence" (2019) 34(3) Intell Natl Secur 362 at 367.
[73] Omand, Bartlett and Miller, above n 6, at 816.

A Intelligence in New Zealand: What are the rights at stake?

The role of intelligence and security agencies are underpinned by two rights. In carrying out activities, agencies must strike a delicate balance between protecting a nation from security threats, while maintaining an individual's human rights such as the right to privacy and the right to be secure against unreasonable search and seizure.[74]

1 Collective Rights:

In a free and democratic society, security is considered to be a prerequisite to ensure that individuals can go about their activities without undue interference.[75] In New Zealand, there is no constitutional right to security. However, New Zealand has ratified the International Covenant on Civil and Political Rights (ICCPR), which provides that states have an obligation to protect the security of people within their territory.[76] Importantly, this includes the duty to protect individuals from "deprivation of life, liberty, or security by third parties operating within the state's territory, such as criminals and terrorist groups".[77] This is reflected in the Act's purpose as New Zealand's intelligence agencies have a fundamental obligation to protect New Zealand's security.

2 Individual Rights:

However, the Government must ensure that the protection of security is consistent with other individual rights that New Zealand citizens exercise. Unlike in other jurisdictions, New Zealand does not have a constitutional right to privacy formally enshrined in the New Zealand Bill of Rights Act 1990 (NZBORA). Instead, privacy rights in New Zealand are governed by both statute, the Privacy Act 2020, and the common law tort of privacy. Further, privacy is considered to be the foundation of many of the rights found in the NZBORA including freedom of movement,[78] freedom of expression,[79] freedom from discrimination,[80] and the right under against unreasonable search and seizure.[81]

---

[74] Cullen and Reddy, above n 1, at [1.4].
[75] At [1.5].
[76] International Covenant on Civil and Political Human Rights 999 UNTS 171 (signed 16 December 1966, entered into force 23 March 1976), art 9; Office of the United Nations High Commissioner for Human Rights Human Rights, Terrorism and Counter-Terrorism (Fact Sheet 32, July 2008) at 8.
[77] Cullen and Reddy, above n 1, at [1.5]; United Nations Human Rights Committee General Comment No. 35 on Article 9 of the International Covenant on Civil and Political Rights (28 October 2014) at [7].
[78] New Zealand Bill of Rights Act 1990, s 18.
[79] Section 14.
[80] Section 19.
[81] Section 21.

3 Intelligence and Security Act 2017: Striking a balance:

At the time of drafting, the Act adopted a rights-based approach by attempting to strike an appropriate balance between privacy and security. The Act followed the recommendations in the 2016 First Independent Review of Intelligence and Security in New Zealand, *Intelligence and Security in a Free Society*.[82] Despite common belief that security and privacy conflict, the report indicated that they were complementary and could both be upheld:[83]

> The government does not have to trade security off against human rights. Security is a human right and the law that protects human rights must be flexible enough to allow a balance to be struck.

B Collection of Publicly Available Information: How does it impact human rights?

The main issue is that the Act's authorisation of the use of publicly available information reflects traditional conceptions of privacy. For many years, privacy has been concerned with the physical distinction between the public and private realm.[84] Under this approach, privacy functions to prevent the disclosure of information from the private realm to the public realm.[85] Accordingly, an invasion of privacy occurs at the specific point in which concealed information is obtained or released to others.[86] In contrast, individuals have no claim to privacy in respect of information that already appears in a public record or is disclosed voluntarily into the public domain.[87] However, this position fails to consider that information that is publicly accessible is capable of taking on a private nature, and can breach an individual's reasonable expectation of privacy.

Firstly, while individual pieces of information about an individual may not be telling, upon being combined and assembled, it can create rich portraits of their overall life.[88] Therefore, while an individual may be comfortable with a single fact about them being disclosed in the public domain, this fact can take on an entirely new dimension when combined with other facts about the individual.[89] This problem with aggregation is becoming more prevalent in today's digital society. Due to the increase in information being posted publicly online,

---

[82] Cullen and Reddy, above n 1.
[83] At [1.5] – [1.7].
[84] Helen Nissenbaum "Toward an Approach to Privacy in Public: Challenges of Information Technology" (1997) 7(3) Ethics Behav 207 at 207.
[85] Daniel Solove "Access and Aggregation: Public Records, Privacy and the Constitution" (2002) 86(6) Minn L Rev 1137 at 1184.
[86] At 1176.
[87] At 1177.
[88] Nissenbaum, above n 84, at 217.
[89] At 217.

agencies are able to easily amass information about an individual to form a revealing image.[90]

Secondly, privacy is about the expectations and norms of the environment within which information is shared.[91] When information is compiled, it involves shifting it from one context to another. This means that information becomes disconnected from the original context it was intended to be shared within.[92] For example, when someone shares information publicly with their friends on Facebook they may expect observation by their peers, but not intensive scrutiny by the State.[93] Thus, by agencies taking this information and utilising it in a different context from which it meant to be broadcast, such as national security, it may become highly inappropriate.

Thirdly, with publicly posted information, there is an "informational asymmetry".[94] To fully participate in a website's service a user often has to create a profile, divulge several pieces of personal information, and consent to the platform's terms of service and privacy policies.[95] However, privacy settings on social media platforms are often not well understood and may be subject to change.[96] This means it is often not clear to the user what they have consented to when using the platform, or the potential future uses of the information.[97] This results in a situation where users may have legally accepted for their information to be public and utilised, without necessarily understanding or endorsing it.[98] This is exacerbated in a security context where it is highly unlikely citizens expect their nation's intelligence agencies to view their information at the time of posting. These issues can be illustrated with the following example.

---

[90] At 217.
[91] Quirine Eijkman and Daan Weggemans "Open-Source Intelligence and Privacy Dilemmas: Is it time to Reassess State Accountability?" (2013) 23(4) Secur Hum Rights 285 at 292.
[92] At 292.
[93] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC R141, 2017) at [11.62].
[94] Rønn and Søe, above n 72, at 371.
[95] Adam Garcia "Socially Private: Striking a Balance Between Social Media and Data Privacy" (2021) 107 IOWA L. Rev 319 at 325.
[96] Law Commission and Ministry of Justice, above n 93, at [11.62].
[97] Rønn and Søe, above n 72, at 366.
[98] At 371.

VI Privacy Issue Illustration: Clearview.

A Clearview:

Clearview AI acts as an apt example of the difficulty in balancing the societal right to public safety with an individual's right to privacy. Clearview AI is a United States software company that collects publicly posted images of people's faces and their identities, and uses facial recognition technology to create a database of individual facial biometric identifiers.[99] Clearview then provides a service where a user who wishes to identify an individual can take a photo of that person, upload it to their website and Clearview will run a search within its database to identify likely matches. Where a match is found, photos of the individual will be displayed with exact links to where they appear online.[100] The database, which scrapes sources from a range of social networks such as Facebook, Instagram and YouTube, holds over 20 billion images of 2.8 billion individuals, each obtained without the individual's knowledge or consent.[101]

In early 2021, the New Zealand Police trialled the software without consulting New Zealand's Privacy Commissioner or obtaining consent from the Police Commissioner.[102] Despite the trial involving 150 searches of police volunteers, and 30 searches of persons of interest, only one individual was successfully identified. Further, the software had difficulty identifying individuals of Māori or Pacific Island descent. The New Zealand Privacy Commissioner did not take action to consider the lawfulness of the use of Clearview's services.

B Right to Public Safety vs Right to Privacy:

Under a human rights framework, the use of Clearview's services are only justified where any benefit provided to public safety does not disproportionately erode other rights. In this case, Clearview asserts their technology is providing substantial benefits to public safety since its establishment, however their aggregation of data also appears to be eroding human rights.

The company claims since its establishment it has assisted law enforcement agencies to identify suspects, victims and witnesses during investigations involving child exploitation,

---

[99] Kashmir Hill "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (online ed, New York, 2020).
[100] Hill, above n 99.
[101] Privacy Commissioner "Controversial AI software raises privacy concerns" (22 July 2020) <www.privacy.org.nz>.
[102] Privacy Commissioner, above n 101.

terrorism and sex trafficking.[103] Across the world, over 600 law enforcement agencies have utilised Clearview's services.[104] In instances where an agency has CCTV or cell phone footage of an incident but is unable to identify the people involved, relevant facial images can be uploaded to Clearview's website to produce likely matches and associated source information.

However, as Clearview's services are used to identify people of interest during investigations, it is fundamental that there is a high accuracy rate. While Clearview's algorithm has been confirmed by official US tests as having an accuracy rate of 99.85%,[105] the company has been criticised following a study conducted by the United National Institute of Standards and Technology showing facial recognition technology is racially discriminatory, resulting in significantly higher false positives for ethnic minorities.[106] This can result in increased false accusations, thereby increasing existing biases within our criminal justice system and eroding individual's freedom from discrimination.[107]

Further, Clearview's services represent a radical erosion of an individual's rights to privacy, especially in online spaces. Following public outcry, several Privacy Commissioners in different jurisdictions instituted investigations into whether Clearview's services breached domestic privacy laws. Throughout each investigation, Clearview maintained the position that its services were both lawful and ethical as images were only collected from publicly viewable pages, and thus did not require consent. However, overwhelmingly, Privacy Commissioners in jurisdictions such as the United Kingdom,[108] Canada,[109] France,[110] and Australia[111] each established that Clearview had neither an appropriate nor legitimate

[103] Office of the Privacy Commissioner of Canada "Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Informaiton and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" (2 February 2021) <www.priv.gc.ca> at [19].
[104] Hill, above n 99.
[105] Clearview AI "Consecutive NIST Test Confirm Superiority of Clearview AI's Facial Recognition Platform" (24 November 2021) <www.clearview.ai>.
[106] Harvard University "Racial Discrimination in Face Recognition Technology" (24 October 2020) <www.sitn.hms.harvard.edu/ >.
[107] Lynch and others, above n 61, at 8.
[108] Information Commissioner's Office "ICO fines facial recognition database company Clearview AI Inc more than 7.5m and orders UK data to be deleted" (23 May 2022) <www. ico.org.uk >.
[109] Office of the Privacy Commissioner of Canada, above n 103.
[110] CNIL "Facial Recognition: the CNIL orders Clearview AI to stop reusing photographs available on the internet" (16 December 2021) <www.cnil.fr>.
[111] Office of the Australian Information Commissioner "Clearview AI breached Australian's privacy" (3 November 2021) <www.oaic.gov.au>.

purpose for collecting personal information. For example, the United Kingdom Information's Commissioner Office (ICO) declared that Clearview breached domestic laws by failing to use the information in a way that is fair and transparent, as individuals would not reasonably expect their personal data to be used for completely unrelated identification purposes.[112] The Canadian Privacy Commissioner went further, stating that Clearview's services were mass identification and surveillance of individuals by a private entity.[113]

C Would it be lawful for New Zealand's agencies to use Clearview?

Under the Act, it is likely that an intelligence agency would be able to lawfully utilise Clearview's services if offered, without requiring a warrant. The information that has been collected by Clearview is publicly available, and Clearview's services could be accessed by any member of the public at any time. However, this position seems unlawful as the aggregation of personal data in this way to assume people's identity breaches reasonable expectations of privacy. Clearview has inappropriately taken user's public information and utilised it for an unrelated purpose for which it was uploaded. At the time of using social networking sites, it is unlikely users would expect their facial images can be collected without their consent by a company for completely unrelated identification purposes.

VII Unreasonable Search or Seizure: Does the use of publicly available information constitute a "search" under s 21 of the NZBORA 1990?

The second human right the Act's current position potentially breaches is the right against unreasonable search or seizure under s 21 of the NZBORA 1990. While the Act grants agencies the power to collect publicly available information, the Act prohibits agencies from conducting a "search" without first obtaining an intelligence warrant as per s 67. Therefore, it is instructive to consider whether piecing together a picture of a person's life, movements and activities from publicly available information would be a "search". If established, this would mean it is an "unlawful activity" and a warrant should be required.

A Definition of "Search":

Under s 21, New Zealand citizens are granted the right to be secure from unreasonable search and seizure.[114] Neither the Intelligence and Security Act 2017, nor the Search and Surveillance Act 2012 defines the term "search". Accordingly, whether the conduct of New

[112] Information Commissioner's Office, above n 108.
[113] Office of the Privacy Commissioner of Canada, above n 103, at [72].
[114] New Zealand Bill of Rights Act 1990, s 21.

Zealand's intelligence agencies in collecting public information constitutes a search is a "fact-specific inquiry", assessed against the way New Zealand Courts have defined it.[115]

In *R v Hamed,* the majority in the Supreme Court did not provide a single definition of search. However, the Court established that in order for there to be a breach of s 21, there must have been an invasion of a "reasonable expectation of privacy".[116] In doing so, the Court adopted the purposive approach as formulated by the Supreme Court of Canada in *Hunter v Southam Inc*.[117] In considering whether an intrusion is unreasonable, the Court held it was necessary to consider the values underpinning s 21.[118] Section 21 aims to protect both personal freedom and dignity from unreasonable and arbitrary state intrusion.[119] This requires a balance between the State and citizen, by "preserving space for individual freedom and protection against unlawful and arbitrary intrusion by state agents".[120]

Blanchard J identified two elements relevant to the inquiry of whether a "search" has occurred. Firstly, the plaintiff must have a subjective expectation of privacy in fact at the time of the intrusion.[121] Secondly, the expectation must be one that society is prepared to regard as reasonable.[122] Following a finding of a search, the majority unanimously held the Court must next consider whether it was unreasonable. This involves an assessment of the degree of intrusion into privacy, the nature or place of the object being searched and the reason why the search took place.[123]

B Does New Zealand's Current Approach to "Search" cover the Collection of Publicly Available Information?

1 New Zealand Case Law:

It has never been considered by a Court in New Zealand or any comparable jurisdiction whether the use of publicly available information by agencies breaches s 21. However, as noted above, it is well-established in New Zealand that state action will be treated as a

[115] *Grant v Police* [2021] NZHC 2297 at [79].
[116] *Hamed v R* [2011] NZSC 101 at [163].
[117] At [10].
[118] At [10].
[119] At [10].
[120] At [10].
[121] At [163].
[122] At [163].
[123] At [172].

"search" if it intrudes on an individual's reasonable expectation of privacy.[124] Thus, privacy has been inherently linked to a s 21 search.[125] In *Hosking v Runting,* Tipping J observed that "the right to be free from unreasonable search and seizure … is not very far from an entitlement to be free from unreasonable intrusions into personal privacy".[126]

While previously limited to private spaces, New Zealand Courts have begun to recognise that a reasonable expectation of privacy can be recognised in public in some instances.[127] Generally, this will occur where surveillance will observe beyond that which can be seen through simple human observation.[128] For example, in *R v Lorigan,* the Court of Appeal held that a camera with night-vision capabilities was a "search" for the purposes of s 21 as the images it could capture "were such that could not be seen by the naked eye".[129] However, ultimately the search was deemed both lawful and reasonable as it was not prohibited by any statute or common law rule and occurred on a public street.[130] Significantly, in *R v Hamed,* Elias CJ established that individuals may be able to maintain a reasonable expectation of privacy in public spaces "if those observed or overheard reasonably considered themselves out of sight or earshot", thus falling within the protections of s 21.[131]

Therefore, it could feasibly be argued that the collection of publicly available information breaches s 21, following the widened approach New Zealand Courts have taken to a "search". This is because agencies can observe beyond what would normally be able to be viewed by any member of the public online through the aggregation of such information. Further, due to the informational asymmetry, users would likely consider themselves "out of earshot" of NZ's agencies at the time of posting.

2 Search and Surveillance Act 2012 Review:

Some of these issues were addressed in 2016 in the Law Commission and Ministry of Justice jointly published Issues Paper which described possible ways to improve the Search and

[124] At [163]; *Lorigan v R* [2012] NZCA 264 at [22].
[125] Lynch and others, above n 61, at [4:9].
[126] *Hosking v Runting* [2005] 1 NZLR (CA) at [225].
[127] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012: Issues Paper* (NZLC IP40, 2016) at [3.105].
[128] Lynch and others, above n 61, at [4.4.3].
[129] At [4:7]; *Lorigan v R,* above n 124, at [25].
[130] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012: Issues Paper,* above n 127, at [3.106]; *Lorigan v R*, above n 124, at [25].
[131] *Lorigan v R,* above n 124, at [12].

Surveillance Act.[132] Amongst other things, the review considered whether warrantless public surveillance methods, which includes accessing social media and internet platforms to obtain publicly available information, requires greater regulation under the Act.[133] The review found the use of publicly available information is commonly used in New Zealand and is largely unobjectionable as officers can only find as much information as any member of the public.[134] However, the report does argue with significant advancements in modern technology, previously lawful utilising of public information has the potential of intruding on reasonable expectations of privacy.[135] For example, technology allows significant volumes of information to be gathered, aggregated and analysed in a way that an individual person could not previously achieve.[136] Ultimately, while the report does not conclude that such monitoring constitutes a search, it left open that previously lawful methods could potentially engage s 21.[137]

During its analysis, the report establishes a number of factors that help indicate whether public surveillance would breach s 21.[138] There are two highly relevant factors; whether the observation of an individual is "casual" or involves "intensive scrutiny",[139] and whether technology is used to enable observation of something that could not otherwise be seen.[140] When using public information, agencies are able to identify and subject individuals to intensive scrutiny that would not ordinarily be anticipated. While individuals cannot control who observes information once released into the public domain, it is unlikely they would expect to be personally identified by agencies and subject to extensive surveillance. Further, agencies are granted the power to monitor the activities of any member of the public, many of whom are law-abiding citizens in which there are no reasonable grounds to capture their activities. Lastly, there is the ability of agencies to aggregate public information to form a

[132] Law Commission "Search and Surveillance Act 2012" (28 June 2016) Law Commission <www.lawcom.govt.nz>.
[133] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012*, above n 93, at [11.4].
[134] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012: Issues Paper,* above n 127, at [3.104].
[135] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012,* above n 93, at [5.4].
[136] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012: Issues Paper,* above n 127, at [3.117].
[137] At [3.118].
[138] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012,* above n 93, at [11.20].
[139] At [11.20].
[140] At [11.20]

picture of a person's life. This means what agencies view is qualitatively different from what an ordinary person would be able to discern from a single piece of information.

C Overseas Approach to "Search": United States Mosaic Theory:

In the United States, the Courts have developed the mosaic theory, a novel approach to address this situation of aggregation. Instead of considering whether a particular act in isolation constitutes a search, the theory assumes that a set of non-searches aggregated together may amount to a search.[141] This is because the collection of individual pieces of a puzzle that may seem small in isolation may be subsequently assembled to create a revealing mosaic of a person, thereby violating an individual's reasonable expectation of privacy.[142]

The Fourth Amendment to the United States Constitution protects an individual's privacy interests by protecting people from unreasonable search and seizures by the government.[143] Similar to s 21 NZBORA, the Fourth Amendment does not guarantee individuals the right against all search and seizures, rather it protects individuals against such government invasions that are deemed unreasonable under the law. Traditionally, the US Court's used a sequential approach to determine whether a "search" amounted to a breach of the Fourth Amendment.[144]

In *Katz v. United States, 88 S. Ct. 507,* the United States Supreme Court introduced a two-prong test to determine whether law enforcement agencies had violated an individual's "constitutionally protected reasonable expectation of privacy". Firstly, a claimant must prove that they exhibited an actual expectation of privacy.[145] Secondly, the expectation must be one that society is prepared to recognise as reasonable.[146] Thus, a search would occur at the point in which the government enters into an individual's private space, even in an area accessible to the public. However, conduct would not violate a reasonable expectation of privacy when it involved observing what has already been exposed to the public.

---

[141] Orin Kerr "The Mosaic Theory of the Fourth Amendment" (2012) 111 Mich L Rev 311 at 320.
[142] At 320.
[143] United States Constitution, amend IV.
[144] Kerr, above n 141, at 312.
[145] *Katz v United States* 389 US 347 (1967) at [361].
[146] At [361].

However, technological advancements in large-scale data collection saw the Courts first apply the mosaic theory in the District Court of Columbia in *United States v Maynard*.[147] In the case, the defendant claimed he had been subject to a Fourth amendment search after a GPS tracking device was installed on his car, tracking his location data for over 28 days.[148] Ginsburg J upheld the *Katz* position, stating whether an expectation of privacy is reasonable depends on whether the expectation relates to information which has been exposed to the public.[149] However, Ginsburg J suggested that instead of inquiring into whether the likelihood of discrete pieces of information would be exposed to the public, it must be considered whether the entire monitoring as a whole would be exposed.[150] While some of the discrete movements of the defendant would have been exposed to the public, the collective monitoring over the 28 days revealed an "intimate picture of the subject's life he expects no one to have".[151] Therefore, Ginsburg J argued the monitoring over time reveals more than what individually would be seen:[152]

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, and what he does not do, and what he does ensemble. These types of information can reveal more about a person than does any individual trip viewed in isolation.

The Supreme Court in *United States v Jones* unanimously upheld that Jones had been subject to a Fourth Amendment search. While none of the Justices explicitly cited the mosaic theory, their approaches taken were similar.[153]

VIII What type of action could be taken?

Overall, it is clear that the Intelligence and Security Act's current position fails to appropriately balance national security with individual's right to privacy and the right to be secure against unreasonable search or seizure. This is an issue that forms part of the current review of the Act, which is due to be presented to the parliamentary Intelligence and Security Committee in late December. This section analyses two potential approaches that the review could consider implementing.

---

[147] *United States v Maynard* 615 F 3d 544 (DC Circ 2010).
[148] At [549].
[149] At [558].
[150] Kerr, above n 141, at 324.
[151] At 326.
[152] At 324.
[153] At 326.

A Policy Statements:

Firstly, the legislative framework of the Act could remain unchanged, however more frequent Ministerial Policy Statements could be issued by the Minister Responsible for the GCSB and NZSIS under s 206 of the Act.[154] This would ensure clear and consistent guidance is provided to the NZSIS and GCSB about what situations the use of publicly available information is considered a lawful activity.

1 Benefits:

The Joint Law Commission and Ministry of Justice review of the Search and Surveillance Act offers some useful insights. Ultimately, the report concluded that the Search and Surveillance Act needed more transparent guidance to regulate the use of public surveillance.[155] The most appropriate mechanism identified was the use of policy statements regularly issued by the Commissioner of Police and Chief Executives on the basis that it would offer flexibility, as they can regularly be updated to deal with new situations as they arise with advancements in technology.[156] In contrast, it was deemed a regime requiring enforcement officers to obtain a warrant for public surveillance was inappropriate and impracticable, as it would create significant compliance burdens on officers when the majority of the surveillance carried out is both routine and lawful.[157] Further, the report argued specific statutory criteria setting out rules about which circumstances various public surveillance methods could be used would not be viable.[158] This is because it would be difficult to identify every circumstance when an individual has a reasonable expectation of privacy. This and technological advancements mean statutory criteria could quickly become outdated and need to be reviewed.[159]

2 Critiques:

However, policy statements do not have the same teeth that changes in legislation do. While Ministerial Policy Statements issued under s 206 of the Act set out the Minister's expectations of how activities should be carried out and what restrictions should be placed on them, they

[154] Intelligence and Security Act 2017, s 206.
[155] Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012,* above n 93, at [11.30].
[156] At [11.35] – [11.36].
[157] At [11.33].
[158] At [11.34].
[159] At [11.34].

do not act as legal authorisation.[160] This means some discretion is left to NZSIS and GCSB employees to ultimately make any decision regarding the use of publicly available information. As the Act is supposed to protect New Zealand citizen's rights and freedoms, an approach that has actual legal ramifications may be more appropriate.

B Law Reform:

Secondly, and more convincingly, there could be potential reform of the Intelligence and Security Act's approach to publicly available information. The mosaic theory could be utilised to underpin the law reform. Under this approach, the aggregation of publicly available information could be defined as an "unlawful activity" under the Act, thereby requiring an intelligence warrant. This would act as an "equilibrium adjustment" by strengthening the protections of individuals in the face of increasing erosion of their rights arising from the Government's enhanced powers.[161]

1 Benefits:

The main benefit that law reform offers is that it ensures clear legal limits are put in place to regulate the increasingly intrusive use of publicly available information. The importance of legal frameworks was made evident in *R (on the application of Bridges) v Chief Constable of South Wales,* a landmark decision of the England and Wales Court of Appeal.[162] While the Court did not consider whether the use of publicly available information by state actors constitutes a "search", the decision illustrates that detailed legislation is the most appropriate mechanism to govern novel state surveillance technologies.

The appeal turned on whether the use of live Automated Facial Recognition Technology (AFR) by the South Wales Police was lawful.[163] AFR is a surveillance device used by police that captures live digital images of people's faces, which are instantly processed and compared with images of persons on a police watchlist.[164] The Court of Appeal established it was unlawful as it interfered with the right to respect for private life under Article 8 of the European Convention on Human Rights.[165] The Court then analysed whether there was a

[160] Andrew Little *Cooperating with overseas public authorities* (New Zealand Intelligence Community, Ministerial Policy Statement, 1 April 2022) at [2].
[161] Kerr, above n 141, at 345.
[162] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
[163] At [1].
[164] At [1].
[165] At [130].

sufficient legal framework governing when and how AFR could be used. Despite the framework comprising a combination of common law principles, legislation, and local police policies, ultimately, the Court held it was insufficient.[166] This was because it left police officers discretionary powers that were too wide as there was no clear guidance on where AFR could be deployed or who was to be placed on the watchlist.[167] Following this line of reasoning, it is fundamental that the Act is updated to prevent intrusive discretion by New Zealand's intelligence agencies in their use of publicly available information.

2 Critiques:

However, there are significant criticisms of the mosaic theory which must be considered before it is used to guide law reform. Firstly, the application of the mosaic theory raises a number of practical issues. The doctrine would require the Act establishes a clear line between aggregation of information that will trigger a reasonable expectation of privacy, and that which it will not.[168] If the legislation is left vague and unpredictable, agencies will not be able to predict with certainty whether their actions during an investigation will violate a reasonable expectation of privacy by creating a mosaic.[169] On one hand, this means that they may frequently violate a search.[170] On the other hand, they may be overly cautious in their investigations, thus limiting their ability to effectively and efficiently conduct intelligence. While it is important that New Zealand's intelligence agencies are restrained and do not violate privacy rights, an approach should not be adopted that limits intelligence service effectiveness and ability to deter security threats.[171]

Secondly, the theory has been criticised on the basis of being logically inconsistent. The theory only operates where information's constituent parts do not implicate reasonable expectations of privacy. However, as raised by Sentelle J, dissenting judge in *United States v Jones,* "the sum of an infinite number of zero-value parts is also zero".[172] Thus, it may be unusual if the Act established there is no expectation of privacy in a specific public movement so no warrant is required, however there can be an expectation in a collection of

[166] At [90].
[167] At [91].
[168] David Gray and Danielle Keats Citron "A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy" (2013) 14 NC JL & Tech 381 at 408.
[169] At 409.
[170] At 410.
[171] Akin Ünver, above n 31, at 17.
[172] *United States v Jones* 625 F 3d 766 (DC Circ 2010) at [8].

these movements.[173] This runs contrary to the traditional approach of a search that New Zealand Courts have considered.

IX Conclusion:

In conclusion, the legislation covering New Zealand's intelligence agencies use of publicly available information is no longer fit for purpose. There is no doubt that open-source intelligence is a useful tool regularly utilised by intelligence agencies to assist in their function of protecting New Zealanders from security threats. However, while the Intelligence and Security Act 2017 clearly authorises agencies to collect, obtain and use public information without requiring a warrant, this position is no longer legitimate as it fails to act in accordance with all human rights obligations. In an age where technological advancements have seen vast volumes of information about individuals' lives publicly uploaded, agencies can use novel techniques to amass and combine information, creating deeply intrusive images of individuals. This has the potential of undermining two important rights; the right to privacy, and the right to be secure against unreasonable search and seizure.

Across the world, the appropriate treatment of publicly available information is being debated by courts and legal authorities, with no authoritative viewpoint being arrived at. In a security context, the question of where the balance should fall between national security and individual's rights is contested, unsettled and open to interpretation. Therefore, the review of the Intelligence and Security Act has come at a critical time. This is an area that requires significant and urgent attention to ensure that the law that is purposefully designed to protect individual's rights is kept up to date with modern technology.

[173] Gray and Citron, above n 168, at 398 – 399.

Word Count:

The text of this paper (excluding table of contents, abstract, non-substantive footnotes, and bibliography) comprises approximately **7728** words.

Bibliography:

A Cases:

1 New Zealand:

Grant v Police [2021] NZHC 2297.

Hamed v R [2011] NZSC 101, [2012] 2 NZLR 305.

Hosking v Runting [2005] 1 NZLR (CA).

Lorigan v R [2012] NZCA 264.

2 United States:

Katz v United States 389 US 347 (1967).

United States v Maynard 615 F 3d 544 (DC Circ 2010).

United States v Jones 625 F 3d 766 (DC Circ 2010).

3 England and Wales:

R (on the application of Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.

B Legislation:

1 New Zealand:

Intelligence and Security Act 2017.

New Zealand Bill of Rights Act 2020.

Privacy Act 2020.

Search and Surveillance Act 2012.

2 United States:

United States Constitution.

C Treaties:

International Covenant on Civil and Political Human Rights 999 UNTS 171 (signed 16 December 1966, entered into force 23 March 1976).

D Books:

Nihad Hassan and Rami Hijazi "Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence" (Apress Berkeley, California, 2018).

E Journal Articles:

Adam Garcia "Socially Private: Striking a Balance Between Social Media and Data Privacy" (2021) 107 Iowa L Rev 319.

Damien Rogers "Intelligence and Security Act 2017: A Preliminary Critique" (2018) 4 NZ L Rev 657.

Daniel Solove "Access and Aggregation: Public Records, Privacy and the Constitution" (2002) 86(6) Minn L Rev 1137.

David Gray and Danielle Keats Citron "A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy" (2013) 14 NC JL & Tech 381.

David Omand, Jamie Bartlett and Carl Miller "Introducing Social Media Intelligence (SOCMINT)" (2012) 27(6) Intell Natl Secur 801.

Gašper Hribar, Iztok Podbregar and Teodora Ivanuša "OSINT: A "Grey Zone"?" (2014) 27(3) Int J Intell CounterIntell 529.

Helen Nissenbaum "Toward an Approach to Privacy in Public: Challenges of Information Technology" (1997) 7(3) Ethics Behav 207.

Joel Reindeberg "Privacy in Public" (2014) 69 Mia L Rev 141.

Kira Vrist Rønn and Sillie Obelitz Søe "Is social media intelligence private? Privacy in public and the nature of social media intelligence" (2019) 34(3) Intell Natl Secur 362.

Margaret Hu "Cybersurveillance Intrusions and an Evolving Katz Privacy Test" (2018) 55 Am Crim L Rev 127.

Orin Kerr "The Mosaic Theory of the Fourth Amendment" (2012) 111 Mich L Rev 311.

Quirine Eijkman and Daan Weggemans "Open Source Intelligence and Privacy Dilemmas: Is it time to Reassess State Accountability?" (2013) 23(4) Secur Hum Rights 285.

F Parliamentary and Government Materials:

Andrew Little *Collecting human intelligence* (New Zealand Intelligence Community, Ministerial Policy Statement, 1 March 2022).

Andrew Little *Cooperating with overseas public authorities* (New Zealand Intelligence Community, Ministerial Policy Statement, 1 April 2022).

Christopher Finlayson *Obtaining and using publicly available information* (New Zealand Intelligence Community, Ministerial Policy Statement, September 2017).

Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012: Issues Paper* (NZLC IP40, 2016).

Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* (NZLC R141, 2017).

Office of the United Nations High Commissioner for Human Rights Human Rights, Terrorism and Counter-Terrorism (Fact Sheet 32, July 2008).

United Nations Human Rights Committee General Comment No. 35 on Article 9 of the International Covenant on Civil and Political Rights (28 October 2014).

G Papers and Reports:

Hamid Akin Ünver *Digital Open Source Intelligence and International Security: A Primer* (EDAM Research Reports, Cyber Governance and Digital Democracy, July 15 2018).

Michael Cullen and Patsy Reddy *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (New Zealand Parliament, 29 February 2016).

Nessa Lynch and others *Facial Recognition Technology in New Zealand Towards a Legal and Ethical Framework* (Law Foundation New Zealand, Wellington, 2020).

Royal Commission of Inquiry into Terrorist Attack on Christchurch Mosques on 15 March 2019 "Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019" (2020).

H Speeches:

Andrew Little, Minister of Health of New Zealand "Intelligence and Security in Our Changing World" (Speech to the Victoria University of Wellington Centre for Strategic Studies, Wellington, 4 November 2021).

I Newspaper Articles:

Kashmir Hill "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (online ed, New York, 2020).

Thomas Manch "More data surveillance and less privacy? Spy chief says the public must decide" *Stuff* (online ed, New Zealand, 12 June 2021).

J Internet Resources:

Clearview AI "Consecutive NIST Test Confirm Superiority of Clearview AI's Facial Recognition Platform" (24 November 2021) <www.clearview.ai>.

CNIL "Facial Recognition: the CNIL orders Clearview AI to stop reusing photographs available on the internet" (16 December 2021) <www.cnil.fr>.

Government Communications Security Bureau "Intelligence Collection" <www.gcsb.govt.nz/>.

Harvard University "Racial Discrimination in Face Recognition Technology" (24 October 2020) <www.sitn.hms.harvard.edu/ >.

Hugh Tomlinson "Case Law: R (on the application of Bridges) v Chief Constable of South Wales, Police use of automatic facial recognition technology unlawful – Hugh Tomlinson QC" (17 August 2020) Inforrm's Blog <www.inforrm.org>.

Information Commissioner's Office "ICO fines facial recognition database company Clearview AI Inc more than 7.5m and orders UK data to be deleted" (23 May 2022) <www.ico.org.uk >.

Law Commission "Search & Surveillance Act 2012" (28 June 2016) <www.lawcom.govt.nz>.

Ministry of Justice "Intelligence and Security Act Review" (2 September 2022) <www.justice.govt.nz>.

Ministry of Justice "Review of the Intelligence and Security Act 2017: Progress Report No 1" (1 August 2022) <www.justice.govt.nz >.

Ministry of Justice "Review of the Intelligence and Security Act 2017: Terms of Reference" (1 August 2022) <www.justice.govt.nz>.

New Zealand Intelligence Community "New Zealand Security Intelligence Service (NZSIS)" <www.nzic.govt.nz>.

Office of the Australian Information Commissioner "Clearview AI breached Australians' privacy" (3 November 2021) <www.oaic.gov.au>.

Office of the Privacy Commissioner of Canada "Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" (2 February 2021) <www.priv.gc.ca>.

Privacy Commissioner "Controversial AI software raises privacy concerns" (22 July 2020) <www.privacy.org.nz>.

Privacy Commissioner "Intelligence and Security Act amendments to Privacy Act: FAQs" (28 September 2017) <www.privacy.org.nz>.

Privacy Commissioner "Principle 2: Source of personal information – collect it from the individual" <www.privacy.org.nz>.

Privacy Commissioner "Principle 3: Collection of information from subject – what to tell the individual" <www.privacy.org.nz>.

Privacy Commissioner "Principle 4: Manner of collection" <www.privacy.org.nz>.