Public Interest Law Journal of New Zealand

(2020) 7 PILJNZ 116

ARTICLE

Digital Strip Search: Privacy Concerns Arising from the Electronic Device Search Provision in the Customs and Excise Act 2018

WINNIE CHAU*

Providing another person access to our electronic devices, such as our smartphones, can be an uncomfortable experience. With the passing of the Customs and Excise Act 2018 (CEA 2018), Parliament introduced a power for Customs officers to search personal electronic devices for evidence of relevant offending. To aid enforcement, the new CEA 2018 also criminalises failure to assist a Customs officer in accessing an electronic device without reasonable excuse. With electronic devices containing vast amounts of personal information, these new provisions set up a battleground of competing values. On one side stands privacy; on the other, law enforcement. I acknowledge that the CEA 2018 provides greater protection for the privacy interest compared to its preceding legislation. However, I argue that the new electronic search provisions still present a significant threat to privacy. Notably, the CEA 2018 does not provide sufficient guidance on conducting electronic searches. There are also only a few mechanisms for individuals seeking redress for breaches of privacy during the electronic search process. In arguing for greater emphasis on the privacy interest, I posit that the principles applying to physical searches should guide electronic searches, which permits only a narrow scope. Moreover, an ex ante approach is appropriate for searching electronic devices, where restrictions on what can be searched are articulated in advance. I also argue against applying the plain view exception when Customs finds evidence of other offending, reducing the potential for a fishing expedition. Finally, I propose search warrants should be required for electronic searches at the border, as doing so would better protect the privacy interest without significantly impeding effective law enforcement.

* BA/LLB, University of Auckland. This article was based on a paper submitted in partial fulfilment of the requirements for LAWHONS 744. The author would like to thank Mr Stephen Penk for his guidance in the drafting of this article.

I Introduction

The smartphone has revolutionised communications and entertainment, practically becoming an extension of our daily lives. Alongside the computer and the Internet, the smartphone has been pivotal in creating a level of interconnectedness never seen before in human history. While bringing a host of benefits to the everyday person—such as convenience, ease of communication, and access to knowledge and information storage—portable electronic devices have also facilitated new ways of committing crime.

The law has been slow to adapt to these technological changes with the Customs and Excise Act 1996 (CEA 1996) being a prominent example. With the border presenting New Zealand's first line of defence, the New Zealand Customs Service (Customs) plays an important role in investigating and preventing potential wrongdoing. However, the outdated CEA 1996 provided no guidance on how Customs should treat digital devices at the border, despite evergrowing numbers of device ownership. Clearly, the CEA 1996 had not kept pace and was in severe need of review.

Parliament's response was to pass the Customs and Excise Act 2018 (CEA 2018), which contains a statutory power for Customs officers to search electronic devices.[1] To aid enforcement, it also criminalises failure to assist a Customs officer in accessing an electronic device without reasonable excuse.[2]

Naturally, a power to demand travellers to turn over digital devices for examination raises significant privacy concerns. The passing of the CEA 2018 has set up another battleground of competing values: on one side stands privacy, on the other, law enforcement. This tension is frequently canvassed in academic commentary, particularly in the context of covert surveillance and government interception of digital communications.[3] In contrast, the search of digital devices has received far less coverage.

As the CEA 2018 came into effect in October 2018, it is relatively new and there is little commentary on its digital search provisions. Therefore, the views put forth in this article have largely been informed by other New Zealand statutes and secondary sources from other jurisdictions. While a few cases have come before the courts under the CEA 2018, none have involved an electronic device search yet and it did not involve an electronic device search yet.[4] Furthermore, there are only two years' worth of Customs data on the number of device searches conducted under the CEA 2018.[5]

A *Structure*

First, to understand the interests at stake with the new CEA 2018, this article will look at the conceptual underpinning of the contest between privacy and law enforcement. Part II will explore relevant definitions of privacy and introduce competing interests that sit

1 Customs and Excise Act 2018 [CEA 2018], s 228.
2 Section 228(8).
3 See Samuel Beswick "For Your (Government's) Eyes Only" [2012] NZLJ 214 at 214–215; Geoffrey Palmer "Privacy and the Law" [1975] NZLJ 747 at 751–752; and Tony Black "Privacy – Why?" [1980] NZLJ 329 at 329–331.
4 See for example *Blue Reach Services Ltd v Spark New Zealand Trading Ltd* [2019] NZCA 2, [2019] NZAR 333.
5 New Zealand Customs Service *Annual Report 2019* (17 October 2019) at 101; and New Zealand Customs Service *Annual Report 2020* (1 December 2020) at 109.

alongside law enforcement. It will also argue for a higher expectation of privacy in relation to personal electronic devices.

Part III will examine electronic device search powers under both the CEA 1996 and the CEA 2018. This discussion will include an overview of search powers under the old CEA 1996, followed by a recap of the journey that the Customs and Excise Bill 2016 took through the parliamentary process.[6]

Part IV will analyse the privacy concerns arising from s 228 of the CEA 2018, which is the provision governing electronic device searches at the border. This Part will begin by introducing key aspects of the CEA 2018 and subsequently evaluate whether each aspect favours privacy or law enforcement interests. Part IV will also present privacy concerns that stem from the gaps in the CEA 2018, as well as provide corresponding solutions that balance privacy and law enforcement interests.

Part V will evaluate how the CEA 2018 interacts with other New Zealand legislation in terms of the clash between privacy and law enforcement. This will involve canvassing key New Zealand statutes, such as the Privacy Act 2020 and the New Zealand Bill of Rights Act 1990 (NZBORA). Part V will also propose legal reforms to better promote privacy interests during electronic device searches.

B *Scope*

The digital search provisions in the CEA 2018 raise questions around the balance between law enforcement and privacy. Due to the complexity of information sharing provisions, this article will not address the multiple provisions governing disclosure of Customs collected information to government and private sector agencies.[7]

Compelling owners of digital devices to provide access to the device's contents raises privilege issues, which the CEA 2018 partly addresses.[8] Various privileges present legal grounds to refuse assisting a Customs officer in accessing particular information contained on a device. The CEA 2018 states that privileges contained in subpart 5 of the Search and Surveillance Act 2012 apply during an electronic device search at the border.[9] While privilege is an important aspect to consider in light of the new CEA 2018, this article will not comment on these issues; instead, it will focus on the privacy aspects of the new CEA 2018. Privilege is an evidentiary matter which deserves separate consideration and research.

The intrusion into seclusion tort that arose from *C v Holland* may present an avenue for device owners who have suffered an intrusion into privacy to seek redress.[10] One element of this tort is intrusion into "seclusion", which includes "intimate personal activity, space or affairs".[11] While acknowledging its potential, this article will not discuss the tort. Rather, it will focus on statutory provisions.

6 Customs and Excise Bill 2016 (209-3).
7 CEA 2018, pt 5 subpart 6.
8 Sections 228(13)–228(14) govern privilege as relating to search of electronic devices. Section 254 provides for what constitutes legally privileged information or documents.
9 CEA 2018, s 228(14).
10 *C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672.
11 At [94].

II Foundations: Conceptual Underpinnings

A *Defining privacy*

Defining privacy is of utmost importance as the definition significantly influences the legal solutions that can be crafted to protect it. However, this is no easy task. There is no single agreed definition of privacy, with commentators proposing various ideas. This Part will discuss various conceptualisations that are useful in the context of an electronic device search at the border.

Some conceptions of privacy focus on values of dignity, autonomy and independence.[12] Edward Bloustein characterises privacy as a "spiritual interest", where an invasion of privacy jeopardises human individuality, liberty and dignity.[13] He warns that a person who is aware that their behaviour and opinions will be scrutinised by others will refrain from truly expressing themselves, restraining autonomy and individuality.[14] Tipping J draws on these ideas in *Hosking v Runting*, noting that privacy is necessary in upholding core human values of dignity and autonomy.[15] Similarly, John Craig views privacy as a necessary condition for leading an independent life in a democratic society, providing a retreat from societal expectations and pressure to conform.[16] Accordingly, Craig's definition situates privacy as a fundamental value underpinning human dignity and the integrity of human society.[17]

Privacy can also be conceptualised as a person's control over access to his or her information and the terms by which this information is shared. Judith DeCew, for example, considers the view that control is an essential component of privacy, including control over information about an individual and control over the individual's ability to make personal decisions.[18] Gebhard Rehm takes a similar approach, defining privacy as the ability to make decisions relating to disclosure of personal information.[19] Ultimately, having such control means that if an individual chooses not to disclose information about themselves, they have the right to be left alone, regardless of whether or not they have anything to hide.[20]

This Part has drawn on only two commonly bundled conceptions of privacy because these definitions are the most relevant in the context of electronic device searches at the border. Individuals typically have a subjective expectation of privacy when it comes to their

12 There are multiple conceptions of privacy. For example, Alan Westin considers privacy as "a voluntary and temporary withdrawal of a person" from society: Alan Westin *Privacy and Freedom* (Atheneum, New York, 1967) at 7. Ruth Gavison, on the other hand, suggests privacy is a "limitation of others' access to an individual": Ruth Gavison "Privacy and the limits of law" in Ferdinand D Schoeman (ed) *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press, Cambridge, 1984) 346 at 350.

13 Edward J Bloustein "Privacy As An Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 NYU L Rev 962 at 1002–1003.

14 At 1003.

15 *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [239].

16 John DR Craig "Invasion of Privacy and Charter Values: The Common-Law Tort Awakens" (1997) 42 McGill LJ 355 at 360.

17 At 361.

18 Judith Wagner DeCew *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, Ithaca, 1997) at 53.

19 Gebhard M Rehm "Privacy in the Digital Age: Vanishing into Cyberspace?" in Daniel Friedmann and Daphne Barak-Erez (eds) *Human Rights in Private Law* (Hart Publishing, Oregon, 2001) 373 at 373.

20 Donna-Maree Cross "Surveillance" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) 155 at 158.

digital materials and expect that highly personal information accessed and stored on their electronic devices will stay private.[21] This first conception of privacy enables autonomy and expressions of individuality, creating a sanctuary where the individual is safe from judging eyes. When this expectation of privacy is stripped away and personal information is exposed to the scrutiny of a Customs officer, personal dignity suffers. The ensuing loss of control over the information accessed by the Customs officer comprises a further invasion of privacy.

B *Competing interests*

Privacy is by no means an absolute right. It often comes in conflict with other rights, values and interests. Largely considered a private interest, upholding privacy may come at the cost of public interests, such as efficient law enforcement and freedom of expression.[22] Richard Posner asserts that giving undue weight to personal privacy can lead to certain consequences, such as economic inefficiency, which might run contrary to the public interest.[23] Privacy also faces an inherent disadvantage as its benefits are "often less tangible, visible, or immediate" than benefits offered by competing interests such as law enforcement.[24] It is important, however, to note the significant public interest in protecting privacy.

(1) Law enforcement

Particularly in the context of electronic border searches, law enforcement is the strongest competing interest to privacy. Law enforcement is a public interest aimed at preventing crime and keeping the public safe from potential threats. Several associated interests that are relevant in the search of electronic devices at borders are national security, detection of crime, and public safety.[25] This article's use of the term "law enforcement" will also capture these associated interests.

The tension between law enforcement and privacy often plays out in a search and seizure context. An individual will have reasonable expectations of privacy in relation to his or her belongings. However, in certain situations, this privacy expectation needs to be abrogated to enable effective crime detection and law enforcement. In such cases, search and seizure is unlikely to be considered "arbitrary interference" to privacy, which is condemned under art 12 of the Universal Declaration of Human Rights and art 17 of the International Covenant on Civil and Political Rights.[26] New Zealand has ratified both international instruments and has codified a similar right to be free from "unreasonable search and seizure" in s 21 of the NZBORA.

---

21 Brandon T Crowther "(Un)Reasonable Expectation of Digital Privacy" (2012) 1 BYU L Rev 343 at 352–353.

22 Daniel J Solove "Conceptualizing Privacy" (2002) 90 Calif L Rev 1087 at 1093–1094.

23 Richard A Posner "The Right of Privacy" (1978) 12 Ga L Rev 393 at 403–404.

24 James Waldo, Herbert S Lin and Lynette I Millett (eds) *Engaging Privacy and Information Technology in A Digital Age* (National Academies Press, Washington DC, 2007) at 340.

25 Stephen Penk "Thinking About Privacy" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) 1 at 21–22.

26 *Universal Declaration of Human Rights* GA Res 217A (1948); and International Covenant on Civil and Political Rights 999 UNTS 171 (opened for signature 19 December 1966, entered into force 23 March 1976).

(2) Freedom of expression

Privacy is most frequently contrasted with freedom of expression in the context of media and publicity. With electronic device searches, however, there is less concern that such a search will impede freedom of expression. Therefore, this article will instead focus on the device owner's ability to express themselves freely in the usage of their personal electronic devices.

Stephen Penk considers the notion of privacy not as a competing interest with freedom of expression, but a necessary condition in upholding autonomy which fosters such freedom of expression.[27] Rehm comments that lack of privacy produces a "chilling effect" on speech and behaviour that deviates from the norm, even if it is perfectly legal.[28] These perspectives reinforce Bloustein's illustration of how individuality and autonomy would be lost in a society that disregarded privacy, with individuals afraid to experiment or challenge dominant discourses.[29] Thus, in the case of digital device searches, the right to freedom of expression is congruent with the privacy interest.

C *Great expectations: data privacy*

The backlash that companies receive over breaches of privacy, such as in the aftermath of the Cambridge Analytica scandal,[30] is a strong indicator of how much individuals value digital privacy. With most electronic devices containing highly personal information, there is a heightened expectation of privacy. This sentiment is well accepted by the Supreme Court in *Dotcom v Attorney-General*, acknowledging that:[31]

> … searches of computers (including smart phones) raise special privacy concerns, because of the nature and extent of information that they hold, and which searchers must examine, if a search is to be effective.

The nature and extent of information held on digital devices are two reasons why a digital device search has the potential to be highly intrusive than other types of search. In conducting an empirical study, Matthew Kugler noted that an electronic device search is perceived as being as intrusive as a strip search or a body cavity search.[32]

First, a digital device search is more intrusive because the nature of information stored on personal electronic devices is likely to be more intimate and sensitive than the contents of a vehicle or bag. A cell phone may hold information pertaining to medical records, sexual orientation, political affiliations and religious views that the owner does not wish to disclose.

Secondly, digital devices hold vast amounts of information about their owners. Cell phones and laptops facilitate numerous activities, including personal interactions, gathering and accessing information, financial transactions and entertainment. The extent of information stored on a digital device means there is a high chance that another person

27 Penk, above n 25, at 6.
28 Rehm, above n 19, at 377.
29 Bloustein, above n 13, at 1003.
30 Nicholas Confessore "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far" *The New York Times* (online ed, New York, 4 April 2018).
31 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [191].
32 Matthew B Kugler "The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study" (2014) 81 U Chi L Rev 1165 at 1167.

going through the device's contents will discover the aforementioned intimate and sensitive information.

Another issue is that a device owner will never know everything contained on their device at any one time. With such large volumes of information stored on a device, there is a reasonable fear another person will find information that the device's owner forgot was on the device or did not know was there in the first place. Orin Kerr also notes that often when users delete information, the information is not in fact deleted but rather stays on the device.[33] Information the device owner intended to delete may have been particularly sensitive, further heightening privacy expectations around personal electronic devices.

Considering these reasons, search of electronic devices can present a violation of privacy and dignity tantamount to that of bodily searches.[34] As such, there is a greater case for protection of digital information stored on personal electronic devices during a border search.

III The Customs Landscape

Having canvassed relevant privacy jurisprudence and other conceptual underpinnings, the following Parts of this article will draw together these strands in analysing the CEA 2018's digital search provisions. Part III will provide a legislative overview and history of digital search powers at New Zealand's borders to contextualise the enactment of the CEA 2018.

A *Search powers at the border*

Due to a difference in circumstances, Customs' border search powers differ from search powers exercised by other public bodies. Customs is tasked with preventing the inflow and outflow of dangerous people and goods within a short timeframe to identify wrongdoing.[35] There is also an additional pressure on Customs to perform their tasks diligently because of the increased international efforts to thwart terrorism.[36] These factors are often cited as justifications for why more invasive search powers are warranted at the border.[37]

An evident illustration of the wider search powers conferred on Customs is the largely warrantless nature of border searches in New Zealand. In comparison, a warrant is typically required before searches of people or property, subject to certain exceptions.[38] According to the border search exception—a principle famously observed in the United States—searches at international borders are considered an exception to the general requirement to execute a warrant.[39] As discussed later, this exception seems to apply in New Zealand. However, it is unclear whether such an exception would be subject to a threshold of reasonable suspicion of wrongdoing, as Tim Cochrane suggests.[40] According

33 Orin S Kerr "Searches and Seizures in A Digital World" (2005) 119 Harv L Rev 531 at 542.
34 Kugler, above n 32, at 1208–1209.
35 New Zealand Customs Service *Statement of Intent 2019-2023* (2019) at 3.
36 Tim Cochrane "Protecting Digital Privacy at the New Zealand Border" [2015] NZLJ 138 at 138.
37 At 138–139.
38 *Dotcom*, above n 31, at [71].
39 *United States v Ramsey* 431 US 606 (1977) at 616–617.
40 Cochrane, above n 36, at 138.

to the Law Commission however, there is no requirement to meet such a threshold if Customs is merely exercising "routine powers of inspection".[41]

Considering both the policy and legal aspects of New Zealand's position on border searches, it is evident that law enforcement is a top priority while privacy is relegated further down the list.

B *Customs and Excise Act 1996*

Much has changed since the CEA 1996 was enacted. In 1996, Parliament would not have contemplated the ability of electronic devices to carry information traditionally recorded only in hard copies. This lack of contemplation was reflected in the CEA 1996, which did not contain any express provisions for search of electronic devices.

Despite a lack of express provisions authorising searches of electronic devices prior to 2018, Customs conducted such examinations regardless. In March 2015, Customs claimed that the CEA 1996 provided authority for search of electronic devices at the border.[42] Presented in a discussion paper reviewing the CEA 1996, Customs asserted that its power under s 151 of the CEA 1996 to examine any goods subject to its control also extended to electronic devices.[43] In justifying the extension of this search power, Customs argued that if its officers could search physical documents, officers should also be able to search electronic documents.[44] Furthermore, according to Customs, there is no threshold needed to be met before exercising this search power.[45] Case law at the time supported Customs' stance that s 151 was intended to confer "the widest possible powers" on Customs officers to promote decisional efficiency and operational autonomy.[46]

Under the CEA 1996, Customs' broad powers to search digital devices clearly tipped the scales in favour of law enforcement objectives and against privacy interests. Notwithstanding Customs' assurance that only a few electronic device searches were conducted at the border under the CEA 1996,[47] their ability to exercise search powers without meeting a legal threshold presented a strong threat to individual privacy. The CEA 1996, however, contained a silver lining. Unlike the CEA 2018, there was no express ability for Customs officers to compel device owners to assist in accessing devices. Likewise, a device owner was not legally obliged to assist Customs to access his or her device.[48] Therefore, there was no penalty for refusing to provide a password or encryption key. Customs argued that this loophole prevented them from effectively carrying out their duty to protect the country's borders and investigate criminal activity.[49]

While hindering Customs' powers of search, the lack of express ability to compel under CEA 1996 afforded greater protection of the privacy interest. It is important to note, however, since there is no detailed information on how Customs conducted device searches during this time, there is no way of knowing if device owners were aware of this

41 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) at [1.5].
42 New Zealand Customs Service *Customs and Excise Act 1996 Review Discussion Paper 2015: Powers* (March 2015) at 131.
43 At 131.
44 At 131.
45 At 132.
46 *R v Baird* HC Auckland CRI-2009-004-13439, 27 May 2011 at [16] as cited in *S (CA712/2015) v The Queen* [2016] NZCA 448 at [20].
47 New Zealand Customs Service, above n 42, at 132.
48 At 133.
49 At 133.

protective loophole. Therefore, it is unknown whether the lack of express ability to compel actually amounted to a silver lining for device owners in practical reality.

C *Customs and Excise Act 2018*

Recognising the need for legislative change, the Customs and Excise Bill was introduced in late 2016. Amongst changes to excise duties and other aspects governed by Customs legislation, the Bill contained what is now s 228 of CEA 2018, a provision imposing a duty for owners of electronic devices to assist Customs officers in accessing devices.[50] Failure to fulfil this duty without reasonable excuse constitutes an offence with a penalty of up to $5,000 on conviction.[51]

In debating the electronic search provisions, several Members of Parliament expressed concern over the potential for intrusion into privacy.[52] For example, Barry Coates MP noted that the significant amounts of personal information stored on digital devices give rise to privacy concerns, particularly if the information were to "fall into the wrong hands".[53]

However, Members of Parliament were generally of the opinion that the Bill represented a desirable balance. The Minister of Customs, the Hon Meka Whaitiri MP, expressed that extensive consultation with the Privacy Commissioner assured the House "that the [B]ill balances the protection of New Zealand with the protection of personal privacy".[54] Ms Whaitiri particularly commended the introduction of the "two-stage search" legal thresholds as addressing privacy concerns.[55] Virginia Andersen MP had similar praises for the Bill, noting that the Bill enabled New Zealand to strike an important balance between the protection of the border against individual rights.[56]

Despite the positive reception from Parliament, this article will argue that CEA 2018 still presents significant privacy concerns.

IV Scrutinising the Customs and Excise Act 2018

A *Key provisions of s 228*

This Part will highlight several key provisions and points of interest in s 228 of the CEA 2018 where privacy and law enforcement interests are in contention.

(1) Relevant offending

Customs may only exercise their electronic search power in investigating "relevant offending", which is defined in s 228(5) as "importation or exportation of any prohibited goods" or "unlawful importation or exportation of any goods" or any offences under the CEA 2018. Confining this search power to "relevant offending" means that a Customs officer may not lawfully search electronic devices for offences solely contained in the Crimes Act 1961. Although not affecting the purpose and operations of the Customs, this

50 Customs and Excise Bill 2016 (209-3), cl 207.
51 CEA 2018, s 228(8).
52 (6 December 2016) 719 NZPD 15554–15555.
53 At 15552.
54 (5 December 2017) 726 NZPD 677.
55 (22 March 2018) 728 NZPD 2563.
56 At 2566.

wording does not facilitate the broader law enforcement interest. This restriction provides a degree of protection for individual privacy by minimising the reasons for which an individual may be stopped and have their devices searched.

(2) Legal thresholds

Taking the Privacy Commissioner's recommendations during the drafting process onboard,[57] a legal threshold for electronic searches was introduced in the Customs and Excise Bill.[58] The CEA 2018 sets out two thresholds, with different powers afforded under each one.

For an initial search, a Customs officer must have "reasonable cause to suspect" that a device owner will, or is about to, commit a relevant offence.[59] If this threshold is met, an officer may conduct a search (either manually or with certain technology aids) and must return the device to its owner on conclusion of the search.[60] This search must not take longer than reasonably necessary, damage the device nor be removed from a Customs-controlled area.[61]

If an initial search provides an officer with "reasonable cause to believe" evidence of relevant offending is contained on the device, a more invasive full search is permitted.[62] Establishing this higher threshold enables the use of technology, which has not been approved by the Privacy Commissioner, and enables copying of data from the device.[63] Additionally, it allows Customs to detain a device for as long as reasonably necessary to conduct the search.[64]

These legal thresholds are a marked improvement from a privacy standpoint. Customs claimed that the CEA 1996 permitted searches even in the absence of establishing a threshold, such as reasonable cause.[65] The CEA 2018 is explicit that such practices are no longer permitted.

(3) Disabling transmitting functions

At the Custom and Excise Bill's first reading, some Members of Parliament were concerned about whether the Bill would permit Customs to access any accounts linked to the device during an electronic border search.[66] Being able to access a device owner's social media accounts, email and internet history via an electronic device search would be a grave invasion of privacy. However, s 228(3) of CEA 2018 clarifies that this is not permitted: in conducting an electronic border search, information "accessible from the device but is not stored in the device" may not be accessed.[67] Accordingly, flight mode must be turned on for both initial and full searches.[68]

57 Privacy Commissioner "Submission to the Foreign Affairs, Defence and Trade Committee on the Customs and Excise Bill 209-1" at [16].
58 Customs and Excise Bill 2016 (209-3), cl 207(2).
59 CEA 2018, s 228(2)(a).
60 Section 228(5) definition of "initial search".
61 Section 228(5) definition of "initial search".
62 Section 228(2)(b).
63 Section 228(5) definition of "full search".
64 Section 228(5) definition of "full search".
65 New Zealand Customs Service, above n 42, at 132.
66 (6 December 2016) 719 NZPD 15554–15555.
67 CEA 2018, s 228(3).
68 Section 228(5) definition of "full search" and "initial search".

Section 228(3) prevents Customs from circumventing the requirement for a warrant before accessing information stored on the Cloud.[69] Prohibiting access to the Cloud during all electronic device searches provides another privacy safeguard. Though potentially frustrating for Customs and police who suspect a device owner has evidence of criminal activity stored on the Cloud, s 228(3) leans away from promoting law enforcement and towards privacy. As nothing in the legislation precludes law enforcement from procuring a warrant to search files on the Cloud, this subsection does not create a significant loophole for criminals to hide incriminating evidence from Customs.

(4) Duty to assist

Under the CEA 1996, there was no power to compel a device owner to provide access to their device. However, if the owner did refuse to unlock their device, Customs would have likely detained the device to be examined by its forensics unit.[70] The CEA 2018 creates a legal obligation for the device owner to provide access and assistance that is "reasonable and necessary".[71] If the device owner has no reasonable excuse for failing to carry out this obligation, the device owner commits an offence.[72] Customs may choose to prosecute the device owner, and if convicted, the owner may face a fine of up to $5,000.[73] This legal obligation is an attempt to incentivise cooperation with Customs, reinforcing Customs' ability to detect and prevent crime. With a possible $5,000 fine looming over their head, it is highly likely that a device owner would unlock their device for a Customs officer. While this additional degree of compulsion aids law enforcement efforts, it may push some device owners to forgo their privacy to avoid a financial penalty. If a device owner still refuses to cooperate, Customs may retain the device and attempt to gain access to it via the Customs' forensic team.[74] This power further emphasises the law enforcement interest as it means a device owner cannot simply pay $5,000 and avoid having their device examined.

The duty to assist in providing access to electronic devices is not unique to the CEA 2018. The Search and Surveillance Act 2012 (SSA) contains a similar duty and penalty for non-assistance. Section 130 of the SSA imposes a duty on "persons with knowledge of computer system or other data storage devices" to assist in accessing data stored on a device. Section 178 of the SSA then criminalises failure to comply with s 130, with a penalty of up to three months imprisonment. While no reference was made to the SSA during Parliamentary debates or explanatory notes to the Customs and Excise Bill, it is likely that s 228 of the CEA 2018 draws from ss 130 and 178 of the SSA. Of the few New Zealand cases where ss 130 and 178 of the SSA have come before the courts, only the Court of Appeal decision in *X v R* and the High Court decision in *Hogg v R* touched upon privacy considerations.[75] Proponents of individual privacy should be pleased that the privacy interest is becoming of greater importance in the legal landscape.

69 The Cloud in this context refers to information not stored locally on a device, but rather, stored and accessed over the internet.

70 New Zealand Customs Service, above n 42, at 133.

71 CEA 2018, s 228(2)(c).

72 Section 228(8).

73 Section 228(8).

74 Section 228(9).

75 *X v R* [2020] NZCA 64, [2020] 2 NZLR 590 at [27]–[30]; and *Hogg v R* [2019] NZHC 1254 at [21]. In *X v R* at [29], Collins J notes that "information stored or accessible" through electronic devices "may be both very extensive and intensely private." Collins J then concludes at [30] that search

(5) Reporting the number of devices searched

Currently, s 438 of the CEA 2018 requires Customs to include the total number of electronic devices searched under s 228 in each year's annual report. While this is a step in the right direction for promoting accountability and transparency, the lack of other disclosure requirements renders s 438 rather unhelpful. Additional disclosure requirements could include a breakdown of how many initial searches were escalated to full searches, which among the offences most often give rise to searches and how many searches yielded evidence of relevant offending. Reporting such information will allow Parliament to consider whether further legislative guidance is required to adequately protect privacy during electronic device searches.

Customs' Annual Reports detail how many searches are conducted each year under s 228 of the CEA 2018. A total of 671 initial searches were conducted between 1 October 2018 and 30 June 2019.[76] This figure fell by more than half—to 317 initial searches—in the period between 1 July 2019 to 30 June 2020.[77] However, full searches increased from 47 to 101 in the same respective time periods.[78] The increased conversion rate of initial to full searches suggests that Customs has become more adept at identifying instances of potential wrongdoing that warrant escalation.

Compared to the 537 devices searched in 2017,[79] Customs' Annual Reports since then provide some assurance that the new search powers have not resulted in a significant increase in digital searches at the border. Customs noted that only 0.002 per cent of total travellers have had their devices searched in accordance with s 228 between July 2019 and June 2020.[80] Interestingly, the reports do not provide further clarity as to how Customs conducts its electronic searches.

Looking at the five highlighted aspects of the CEA 2018, the introduction of s 228 is a major step in the direction of upholding privacy interests. Compared to the broad search powers conferred by its predecessor, the electronic search provisions now codified in s 228 have generally acknowledged the privacy interest in electronic devices. However, despite Parliament's best intentions and attempts, this article argues that Parliament has not gone far enough to protect privacy.

B *Issues with the CEA 2018*

This Part will examine privacy issues stemming from the gaps in the CEA 2018 and will put forth recommendations aimed at better protecting the privacy interest.

---

warrants relating to cell phones be as specific as reasonably possible. In *Hogg v R*,, Wylie J briefly refers to the District Court judge's observation "that there is a strong privacy interest in information contained on personal electronic devices".

76 New Zealand Customs Service *Annual Report 2019*, above n 5, at 101.

77 New Zealand Customs Service *Annual Report 2020*, above n 5, at 109.

78 New Zealand Customs Service *Annual Report 2019*, above n 5, at 101; and New Zealand Customs Service *Annual Report 2020*, above n 5, at 109.

79 Seth Rosenblatt "New Zealand defends its border device search policy (Q&A)" (15 October 2018) The Parallax <https://the-parallax.com>; and James Griffiths "New Zealand: Hand over phone password at border or face $3,200 fine" (3 October 2018) CNN International <https://edition.cnn.com>.

80 New Zealand Customs Service *Annual Report 2020*, above n 5, at 109.

(1) Lack of proportionality

An electronic search power currently applies in the same way to all relevant offending under the CEA 2018, regardless of the alleged offence's degree of seriousness. Hypothetically, a Customs officer who suspects an individual of making a false declaration has just as much cause to subject the individual to a device search as an individual suspected of importing illegal firearms.

Considering how intrusive electronic searches are, Jillian Bates proposes that such searches should be conducted only where there is a real threat of serious crime, such as terrorism or conspiracies to import drugs or contraband.[81] She argues that electronic searches for minor crimes is excessively intrusive and may result in commonly marginalised groups facing an increased likelihood of having their privacy intruded upon.[82] Bates recommends imposing limits on the extent of a device search if the suspected offence is a minor offence.[83] This proposed proportional approach would better uphold privacy because suspects of minor offending will be subject to a less intrusive search. However, categorising offences as major or minor may be difficult as drawing the line might be an arbitrary exercise.[84] Furthermore, it will likely be difficult to determine the extent of searches permitted within each category.[85] Even if possession of cannabis and using unlawful travel documents were both classified as minor offences, for example, the information that a Customs officer would search for would differ for each offence.

(2) Search guidelines

Section 228 of the CEA 2018 provides a legal foundation for conducting electronic device searches at the border. However, the CEA 2018 is silent on how to conduct the actual search itself and no cases considering this issue have been brought before the courts yet. This shortage of legislative guidance creates a serious issue for privacy.

To arrive at a suitable method for conducting electronic searches, it is pertinent to consider the jurisprudence of "containers" during a physical search and analyse how this applies in a digital search context.[86] For physical searches without warrant, objects to be searched are typically conceived of as "containers".[87] This manifests in different forms: a vehicle is a container, as is a bag and a safety deposit box.[88] A person being searched may have differing expectations of privacy for each container, which constrains the scope of a warrantless search.[89] For a search of an electronic device, is the cell phone itself one container or does the cell phone consist of numerous containers—that is, the separate files? The first approach would justify the search of all information contained on a device so long as the owner consents to an electronic search. If a broad search were justified under this approach, a search for evidence of one suspected offence may quickly turn into a fishing expedition, which is hardly conducive to privacy. Adopting the views expressed

81 Jillian A Bates "The Forensic Digital Search of Cell Phones at the Border in *United States v Kolsuz*: Tough on Terrorism or Tough on Petty Crime?" (2018) 41(1) NC Cent L Rev 39.
82 At 44–45.
83 At 44.
84 Kerr, above n 33, at 581.
85 At 581.
86 Michael Mestitz "Unpacking Digital Containers: Extending *Riley*'s Reasoning to Digital Files and Subfolders" (2017) 69 Stan L Rev 321 at 326–328.
87 At 326–328.
88 At 326–328.
89 At 324.

by Michael Mestitz in light of the United States Supreme Court's decision in *Riley v California*,[90] this article argues for the latter approach that the cell phone consists of numerous containers.

Mestitz's approach views cell phones as containing numerous folders and files, each a separate container of its own.[91] Each file may also have subcontainers nested inside and according to this concept, each file has an individual expectation of privacy.[92] Therefore, Mestitz argues that a single incriminating file should not justify a broad search of all files contained on a device, such that it is a "drop poisoning the ocean".[93] A Customs officer searching for evidence of one offence would not have free rein to search the device.

Such an approach is necessary to give effect to the NZBORA. As the CEA 2018 is silent on the extent of the search permitted when a Customs officer suspects relevant offending, the digital search provisions should be read consistently with the NZBORA as much as possible.[94] In upholding the right against unreasonable search and seizure, as well as the associated privacy interest, a consistent reading would require New Zealand courts to constrain the extent of an electronic search. Viewing individual digital files as separate containers would enable the courts to fashion clear legislative guidance for how to balance the privacy and law enforcement interests. Mestitz's approach relieves the pressure on Customs officers to perform this balancing act on an ad hoc basis.[95] This is particularly relevant as not every Customs officer will have received legal training and may not be well equipped to engage in such a legal exercise. In contrast, viewing the device as the sole container and consequently justifying a broad search of the device's entire contents would not provide a sufficient safeguard for protecting privacy interests. Therefore, this article argues for limiting the extent of an electronic search until the courts are able to provide further guidance. This article also posits that the courts should approach virtual files as individual containers, in the sense that Mestitz articulates, to best uphold privacy interests.

If a Customs officer is not permitted to search the entire device, how should the officer conduct the search? Kerr proposes two approaches to searching an electronic device.[96] The first is an ex ante approach, where restrictions on what can be searched are articulated in advance.[97] The second is an ex post approach, where restrictions are placed by a judge post-search in determining the admissibility of evidence.[98]

Kerr contends that an ex ante approach is inappropriate as it assumes that judges have the knowledge needed to outline a search strategy before the search commences.[99] In reality, "the forensics process is too contingent and unpredictable" to articulate rules in advance.[100] Kerr also notes that judges lack the technical expertise required to lay out effective search protocols that are appropriate in the particular circumstances.[101] Considering the flaws of such an ex ante approach, Kerr advocates for the ex post approach. He considers that the court's ability to bar disclosure of evidence that is

90 *Riley v California* 573 US 373 (2014) as cited in Mestitz, above n 86.
91 Mestitz, above n 86, at 337.
92 At 341.
93 At 341.
94 New Zealand Bill of Rights Act 1990 [NZBORA], s 6.
95 Mestitz, above n 86, at 350.
96 Kerr, above n 33, at 535.
97 At 535.
98 At 535.
99 At 571.
100 At 572.
101 At 575.

retrieved from beyond the scope of a permissible search would protect the privacy interest.[102]

This article respectfully disagrees with Kerr's perspectives. First, the ex post approach does not protect a person's privacy, as defined in Part II of this article. Going upstream to when the search is first conducted, an ex post approach would permit a Customs officer to conduct a limitless search of the device's contents. Merely having another person see personal and intimate information is enough to trigger feelings of humiliation and a violation of dignity, which are key indicators of an invasion of privacy. Secondly, ex post restrictions would achieve the exact concerns raised by Roberts CJ in *Riley v California*—the sweeping in of large volumes of information.[103] It is only with an ex ante approach that the volume of information exposed to the eyes of a Customs officer may be minimised, in turn protecting the privacy interest. Thirdly, while acknowledging that it may be difficult to ascertain prior to search whether information is relevant, this article submits that there is a solution to balance law enforcement and privacy.

This solution would be to confine a search to locations reasonably thought to contain evidence of the relevant offence that first gave rise to the search. Introducing this rule to limit the scope of an electronic search could only decrease the amount of personal information exposed to a Customs officer. Naturally, a search based on a single criterion—that of reasonable cause to believe a file contains evidence of relevant offending—will feature a smaller pool of information, as opposed to a limitless search of the entire device. A threshold of reasonable cause would, therefore, better protect personal information irrelevant to the alleged offending from being accessed.

In *Riley v California*, Roberts CJ expressed his concern over empowering officers to search locations thought to contain evidence of reasonable offending, stating that "officers would not always be able to discern in advance what information would be found where".[104] He further comments that such a rule would "sweep in a great deal of information", which would be contrary to the privacy interest.[105] Regarding the first concern, if an officer finds it too difficult to discern which locations and files may contain evidence of relevant offending without opening them, there is no reason not to deploy a technology aid to assist with this task. An aid could scan the contents of the device, seeking out information potentially relevant to a certain offence. With a technological aid, there is less private information being exposed to the eyes of another human being. The dignity aspect of the privacy interest is therefore better preserved than if an officer physically opened all files potentially containing relevant evidence.

Other technological search methods, such as hashing, could also be used to similar effect.[106] Kerr explains that intelligence authorities collect common hash values for various types of images or files (such as for child pornography).[107] Running the hash function, an officer would be able to identify matches between hash values held on a database and files located on a digital device without opening the files themselves.[108] This would provide the officer with a degree of confidence that a certain file contains evidence of relevant offending and would satisfy the threshold of "reasonable cause".[109] The derived results

102 At 583.
103 *Riley v California* 573 US 373 (2014) at 399.
104 At 399.
105 At 399.
106 Kerr, above n 33, at 541.
107 At 546.
108 At 546.
109 CEA 2018, s 228(2)(a).

would provide a basis for reasonable cause to search a particular file and restrict the information that an officer physically examines. A criterion of reasonableness offers a way for Customs officers to target the efforts of their manual search to files more likely to contain evidence of relevant offending. This then minimises the potential of intruding into intimate affairs unrelated to offending. Ultimately, this solution strikes a workable balance between effective law enforcement and individual privacy.

(3) Handling evidence of another offence

An officer searching for evidence of one relevant offence may stumble across evidence of another offence. Can the officer then continue to search the device for evidence of this new offence? As there is no legislative guidance, nor information from Customs as to how searches are conducted, this article will consider possible approaches and their respective impacts on privacy.

One approach that Customs may take is the "plain view exception".[110] During traditional searches of places and vehicles, anyone exercising a search power may seize items found "as a result of observation".[111] Though highly simplified here, this is known as the "plain view exception". The Court of Appeal in *Roskam v R* noted that a person exercising search powers may seize items reasonably believed to be evidence of *any* criminal offence.[112] This exception is not confined to seizing evidence of the offence which first gave rise to the search.[113] So long as the searching officer has seen the container before the search power has been completely exhausted, the officer may seize the container and search its contents.[114] However, once the search power has been exhausted for the purpose of seizing items related to the original offence, the searching officer cannot search for any other items believed to be linked to other offences.[115]

Despite the different circumstances and policy considerations involved during an electronic border search,[116] Customs may favour adopting such an approach. Not only is the plain view exception consistent with recent case law and the SSA, but it also makes it easier for Customs to uncover evidence of other relevant offending. This enables Customs to better achieve their law enforcement and crime prevention objectives, though at a cost to individual privacy. Mestitz suggests that adopting the digital container approach (discussed in the previous section) does not preclude the plain view exception from being legitimate.[117]

In contrast, this article argues that taking a plain view exception approach is inappropriate. Within an electronic search setting, such an approach would permit a Customs officer to search for evidence of one offence and collect evidence of other offending up until the officer was satisfied that sufficient evidence of the original offence had been collected. This would create significant privacy concerns due to the volume of information that could be combed through, as well as the potential for a fishing expedition.

110 Mestitz, above n 86, at 350–351.
111 Search and Surveillance Act 2012, s 123(2).
112 *Roskam v R* [2019] NZCA 53, [2019] 3 NZLR 82 at [32].
113 At [32].
114 At [28].
115 At [33].
116 The judgment in *Roskam*, above n 112, discusses the plain view exception arising from a search of a premise conducted under warrant.
117 Mestitz, above n 86, at 350.

A middle ground may be to allow the plain view exception so long as the contents of the digital container are readily ascertainable without opening the container.[118] Under this approach, a Customs officer would be able to open a folder with thumbnails of indecent publications or incriminating file names.[119] This middle ground is not without its limitations, however. Few offenders are likely to leave such clear and obvious indicators of offending. The few who do are likely to be unsophisticated offenders acting individually and this middle ground will often fail to detect large and complex criminal operations. Due to this unsatisfactory nature, this article will instead propose that the appropriate balance between law enforcement and privacy is struck by obtaining warrants for digital device searches.

C *A case for securing a warrant*

While this Part has already proposed three broad suggestions to better uphold the privacy interest within the framework of s 228 of the CEA 2018, this article will also present a case for removing this provision. This radical solution would see this entire provision repealed, instead requiring Customs to secure a warrant before searching any digital devices.

The Supreme Court in *Dotcom v Attorney-General* noted that a search warrant serves the purpose of delineating the legitimate scope of a search.[120] With special concern for the large amounts of information stored on electronic devices, the Court noted that sorting relevant information from irrelevant information "onsite may be impracticable and highly intrusive".[121] Establishing the scope of a search would therefore be best left to a judge, as discussed previously.

A compelling reason as to why this article proposes requiring warrants for electronic searches is that an electronic border search is largely ineffective at deterring crime.[122] With a lower law enforcement interest, the policy reasons exempting warrants for border searches hold less weight. Cochrane explains that objectionable material and information tending to incriminate a person is far more likely to be accessed via the Internet, rather than being stored on a device.[123] As Customs is not permitted to access the Cloud during electronic searches, offenders could simply keep all incriminating evidence on the Cloud. Customs would then have to produce a warrant to access information stored on the Cloud.[124] Robert Diab also notes that the state's interest in performing an electronic search at the border is less compelling than the interest in performing a bodily search: alongside regular examinations of luggage, a body search is the only other way for Customs to prevent entry and exit of narcotics.[125] By contrast, any incriminating evidence stored on a device could be sent via the Internet, leading to a lesser interest in electronic searches.

This article also proposes that if a warrant is required to access Internet communications located on servers, it would be illogical not to have a warrant where the

118 At 351.

119 For example, a folder with a thumbnail icon depicting child pornography was considered searchable under the plain view exception in *United States v Williams* 592 F 3d 511 (4th Cir 2010) at 516–521.

120 *Dotcom*, above n 31, at [71].

121 At [193].

122 Cochrane, above n 36, at 141.

123 At 141.

124 CEA 2018, ss 225 and 228(3).

125 Robert Diab "Protecting the Right to Privacy in Digital Devices: Reasonable Search on Arrest and at the Border" (2018) 69 UNBLJ 96 at 122.

Internet communications are stored on a device crossing the border. The number of warrants that will need to be issued is not likely to be a concern: as mentioned, only a small number of devices are searched each year, with less than 0.002 per cent of all travellers entering and exiting the country being subject to searches between July 2019 to June 2020.[126] Given that so few electronic device searches are conducted at the border, requiring Customs to obtain a warrant for searches would not create an undue burden.

Though obtaining a warrant may take time, this does not impede Customs' ability to investigate potential wrongdoing. One traditional justification for the warrantless border search is that the item being searched could be used as a weapon to harm a Customs officer or to assist in a suspect's escape.[127] However, the United States Supreme Court in *Riley v California* dismissed this reasoning as it applies to electronic device searches, stating that digital information sitting on a device could not be used to aid either objective.[128]

Proponents of warrantless searches also contend that swift action must be taken on intercepting a digital device in order to avoid the possibility of co-conspirators remotely wiping or encrypting devices upon discovering their compromise. It was noted in *Riley v California*, however, that there were operational solutions to prevent remote access from occurring, such as removing a device's battery or placing devices into Faraday bags to isolate them from radio waves.[129]

Requiring Customs to obtain a warrant before conducting an electronic search would afford greater protection for privacy. This requirement would not hinder effective law enforcement, nor create an unnecessarily heavy administrative burden. Accordingly, this article concludes that the CEA 2018 should be amended, prohibiting warrantless searches of electronic devices at the border.

V Clash of the Statutes: CEA 2018 versus the Privacy Act 2020 and the New Zealand Bill of Rights Act 1990

A *Privacy Act 2020*

As the strongest statutory acknowledgement of the privacy interest, this Part will explore how the Privacy Act interacts with the CEA 2018. With numerous inconsistencies between the two statutes, s 228 of the CEA 2018 clearly engages a clash between privacy and law enforcement. This Part will also discuss the current inadequacies of the Privacy Act in the electronic device search context, as well as which statute should prevail over the other.

The Privacy Act imposes legal obligations related to collection and handling of personal information by public and private agencies. Customs is clearly caught by this legislation as it meets the definition of "agency" in s 7(1) of the Privacy Act. Much of the information accessed by Customs during a device search will fall under the definition of "personal information", which is defined as "information about an identifiable individual".[130] Photos and personal records are two examples considered as personal information, which are accessible from an electronic device.

126 New Zealand Customs Service *Annual Report 2020*, above n 5, at 109.
127 *Riley v California*, above n 103, at 386–387.
128 At 387.
129 At 390–391.
130 Privacy Act 2020, s 7(1) definition of "personal information".

(1) Information privacy principles

The Privacy Act contains thirteen information privacy principles (IPPs) that apply to the collection, use and disclosure of information in New Zealand.[131] Section 228 of the CEA 2018 is inconsistent with several IPPs, suggesting that the electronic search provisions lean towards favouring the law enforcement interest over individual privacy. This Part will highlight the more significant inconsistencies.

In the Privacy Act, IPP 2 refers to the "[s]ource of personal information", IPP 3 refers to the "[c]ollection of information from subject" and IPP 4 refers to the "[m]anner of collection of personal information".[132] Section 28 of the Privacy Act stipulates that "IPPs 2, 3, and 4(b) do not apply to personal information collected by an intelligence and security agency." Since Customs is considered an "intelligence and security agency" under s 7 of the Act, s 28 will be engaged in most search and seizure contexts. As such, Parliament has provided a clear mandate that law enforcement objectives should abrogate privacy interests as far as IPPs 2, 3 and 4(b) are concerned. While acknowledging Parliament's express intent to exclude IPPs 2, 3, and 4(b) in a security context, it is still worth exploring the friction between these IPPs and CEA 2018. Doing so will highlight just how much the individual privacy interest suffers as a result of Parliament's legislative intent to favour law enforcement interests. This Part will proceed to analyse the conflicts between CEA 2018 and the IPPs.

The greatest conflict between the CEA 2018 and the IPPs is prima facie contained in IPP 4(b). This principle mandates that personal information should not be collected via unfair or unreasonably intrusive methods.[133] As personal electronic devices contain highly sensitive information, collecting information about an individual by combing through their device—regardless of whether the individual has consented to a search—may be quite intrusive. However, as explained in Part IV, technology aids and processes may be used to comb through information held on the device during a full search,[134] which may limit exposure of highly personal or embarrassing information if it is irrelevant to the offending. The statute's authorisation of a manual examination of a device during the initial search—when such technology limiting exposure of sensitive information is available—could, therefore, possibly be construed as unreasonably intrusive.

A search of a person's cell phone reveals information about not only the individual concerned, but also about his or her friends, families, and other people with whom he or she interacts. Inevitably, information about these people will be indirectly collected. However, IPP 2 establishes that personal information about an individual must be collected directly from the individual.[135] Collecting information indirectly also raises difficulty in complying with IPP 3. This principle specifies that, amongst other requirements, individuals are to be notified of what information is collected, the purpose for collection, and their rights relating to access and correction of information.[136] Collecting information indirectly about person A through searching person B's device may also be unfair on person A. For example, the information about person A on person B's device may paint A in a false light or disclose information exchanged between the two in

131 Section 22.
132 Section 22 (emphasis omitted).
133 Section 22. See information privacy principle [IPP] 4(b).
134 CEA 2018, s 228(5) definition of "full search".
135 Privacy Act, s 22. See IPP 2(1).
136 Section 22. See IPP 3(1).

confidence. This also conflicts with IPP 4(b)'s requirement to collect information fairly, as well as with IPP 2's requirement for information to be collected directly from the person concerned.

Section 228 of the CEA 2018 does not impose obligations for an officer to inform the individual concerned what information is being collected about them, which contravenes IPP 3 of the Privacy Act. While there is no power to collect and store information gathered from a device during an initial search, a full search permits Customs to copy any information deemed necessary.[137] There is no requirement for Customs to inform individuals subject to a full search as to what information will be copied from their device. A lack of such notification decreases transparency and accountability, ultimately harming an individual's chances of seeking legal redress. IPP 3 does not expressly stipulate that an agency must notify an individual as to what personal information is being collected. However, IPP 3(1)(a) requires an agency to notify an individual of "the fact that the information is being collected". This provision would not make sense if the agency was not required to disclose what information was being collected in the first place.

In an electronic search setting, Customs is also unlikely to observe IPP 8, which requires an agency holding personal information not to use this information without first checking its accuracy.[138] For efficiency reasons, an officer is unlikely to ask the individual concerned to check if every piece of information of interest is accurate and not misleading. While a proponent of the individual privacy interest could argue that this omission would be a breach of IPP 8, Customs could argue that it does not yet "hold" personal information at the time of search so IPP 8 does not apply. A narrow reading of the Privacy Act would be required to sustain Customs' argument.

As a partial remedy to the inconsistencies between the CEA 2018 and the Privacy Act, the Privacy Commissioner could issue a code of practice for Customs.[139] This could modify or replace IPPs considered too stringent or inappropriate in an electronic search setting. Thus, curing some inconsistency between the two statutes. For example, a code of practice may recognise the need for efficiency during an electronic search and alter the application of IPP 8 so Customs may collect information without first checking its accuracy with the device's owner. Issuing a code of practice could also enable the Privacy Commissioner to "prescribe procedures for dealing with complaints alleging a breach of the code".[140] Establishing a clear-cut procedure would greatly assist device owners in seeking information about the complaints process, though it may not help substantially in the process of seeking legal redress.[141] Codes of practice may be amended or revoked at any time by the Commissioner, enabling flexibility in striving to balance privacy and law enforcement.

(2) Interference with privacy

Where an IPP is breached, an individual may have a basis for claiming interference with privacy. This Part will discuss potential difficulties with seeking remedies where privacy has been intruded upon during an electronic device search. Establishing interference is an important first step in seeking remedies under the Privacy Act.

137 CEA 2018, s 228(5) definition of "full search".
138 Privacy Act, s 22. See IPP 8.
139 Section 32(1).
140 Section 32(4)(c).
141 Codes of practice may not affect Parts 8 or 9 of the Privacy Act, which pertain to complaints and the proceedings of the Commissioner.

Governed by s 69(2) of the Privacy Act, an interference with privacy must feature two elements. A claimant must first demonstrate that the agency breached an IPP,[142] and must also prove that they suffered harm because of this breach.[143] This could include loss or injury, adverse impact on rights and privileges, or significant humiliation and loss of dignity.[144] If a claimant can meet certain thresholds of harm flowing from an interference with privacy, various remedies are available. However, there are several issues with this avenue of redress.

First, this article contends that the threshold for harm that a complainant must establish is set too high. Under s 69(2)(b)(iii), a complainant must demonstrate "*significant* humiliation, *significant* loss of dignity, or *significant* injury to the [complainant's] feelings".[145] Compared to other categories of harm in the Privacy Act,[146] this category of harm most likely results from an electronic device search. Unless there is widespread publication of information collected during a device search or there is outrageously poor conduct from the Customs officer conducting the search, it is difficult for a complainant to meet this "significant" threshold.

This article views a threshold of "substantial" humiliation, loss and dignity as more appropriate. Tipping J in *Hosking v Runting* proposed the use of "substantial level of offence" as an alternative to a "high level of offence".[147] This is because "substantial" is more flexible than "high level", which may be an unduly restrictive threshold in certain circumstances.[148] Putting aside the context of offensiveness as an element of the public disclosure tort, his Honour's discussion about the relevant threshold of harm is pertinent in discussing remedies under the Privacy Act. Although the standard required under s 69(2)(b)(iii) is "significant" (as opposed to "highly"), this article argues that "significant" is still a higher threshold than "substantial". Adopting the lower threshold suggested by Tipping J may enable victims of overly intrusive device searches to seek legal recourse for loss of dignity and humiliation. Arguments could be made for an even lower threshold in the context of electronic searches, but this new threshold will need to be high enough to discourage litigation over low levels of harm.

The second issue is that many complainants will not be granted a satisfactory remedy. There are multiple layers that a complaint must go through before damages are awarded. The Privacy Commissioner, who investigates complaints and alleged interferences with privacy, has no ability to award damages.[149] If the Privacy Commissioner cannot resolve a particular complaint, he or she may refer the matter to the Director of Human Rights Proceedings,[150] who then decides if the complaint should be heard by the Human Rights Review Tribunal (HRRT).[151] The remedies available in s 102 of the Privacy Act will apply only if the HRRT finds the agency has interfered with privacy. This funnel approach means that only a few complainants who make a claim will receive a remedy.

142 Privacy Act, s 69(2)(a).
143 Section 69(2)(b).
144 Section 69(2)(b).
145 Section 69(2)(b)(iii) (emphasis added).
146 Sections 69(2)(b)(i) and 69(2)(b)(ii).
147 *Hosking v Runting*, above n 15, at [256].
148 At [256].
149 Stephen Penk "The Privacy Act 1993" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) 53 at 70.
150 Privacy Act, s 94(4)(a). See s 7 definition of "Director".
151 Section 97.

Section 102 remedies include a declaration that the agency's action is an interference with privacy, an order restraining the agency from similar action in the future, and an order that the agency take steps to remedy and redress.[152] While the other remedies may be suitable forms of redress for a complainant (depending on the circumstances of the interference with privacy), damages is an inadequate remedy in the electronic device context. An individual who has suffered an interference with privacy due to a Customs officer sifting through the information on their device has suffered a spiritual harm.[153] Paying an amount of money in damages does not seem an appropriate way to compensate for humiliation or injured feelings, which will have already been experienced by the time damages are awarded. Even if an individual were to be satisfied with damages, the amounts awarded by the HRRT have been fairly modest, though recent amounts have been more significant where the complainant suffers a high level of harm.[154] Damages awarded under s 103 are solely compensatory in nature, which is reflected in the amounts awarded.

Improving mechanisms for recourse will enhance the credibility of electronic searches at the border.[155] Other recommendations for improving privacy protections under the CEA 2018 could include requiring Customs officers to inform individuals, whose devices have been searched, on how to lay a complaint with the Privacy Commissioner. These mechanisms will aid in dispelling some apprehension towards s 228 that stems from concern about individual privacy.

(3) Reconciling the Privacy Act with the CEA 2018

Considering the inconsistencies between the CEA 2018 and the Privacy Act, this Part will discuss which statute is likely to be upheld by the courts. During the parliamentary debates over the Customs and Excise Bill, Parliament was clearly cognisant of the significant privacy interests engaged during an electronic device search. As outlined in Part III of this article, many Members of Parliament have acknowledged the Bill as striking a satisfactory balance between privacy interest and law enforcement. In light of this, Parliament must have intended that the privacy interest would be compromised in some ways to allow for effective law enforcement and crime detection. As such, the courts will likely consider that the CEA 2018 will prevail over the Privacy Act. Furthermore, the maxim of *generalia specialibus non derogant* provides that the specific legislation of the CEA 2018 should prevail over the provisions contained in the general Privacy Act.[156]

B *New Zealand Bill of Rights Act 1990*

The NZBORA is another important piece of legislation to consider, though it currently provides little protection for privacy in an electronic device search context.

152 Sections 102(2)(a)–102(2)(b) and 102(2)(d).

153 See generally, Bloustein, above n 13, at 1002–1003 defining privacy as a "spiritual interest".

154 As in *Hammond v Credit Union Baywide* [2015] NZHRRT 6, where the complainant was awarded $98,000 for humiliation, loss of dignity and injury to feelings. The complainant suffered widespread harassment and loss of employment, a severe harm reflected in the amount awarded to her.

155 Waldo, Lin and Millett, above n 24, at 331.

156 *Generalia specialibus non derogant* is a maxim of statutory interpretation stipulating that a specific provision should prevail over a general provision if there is conflict between two laws.

It is unlikely that a device owner would be able to point to an inconsistency with the NZBORA as a reason to invalidate the CEA 2018 or seek a remedy. Notably, the NZBORA does not include a right to privacy. Several complementary rights are codified, including the right to be free from unreasonable search and seizure,[157] right to freedom of association,[158] freedom of expression,[159] and the right to freedom of thought, conscience and religion.[160] These are not particularly helpful in an electronic search setting. The express provision in s 228 of the CEA 2018 permitting device searches means that a search will seldom be unreasonable provided that the requisite threshold is met. The other rights would likely arise indirectly out of the possible chilling effect that a potential electronic search at the border would create on society. Therefore, a potential claimant seeking a declaration of inconsistency or any other remedy would struggle to demonstrate inconsistency.

Even if the electronic search provisions in the CEA 2018 were deemed inconsistent with the NZBORA, the CEA 2018 will prevail over the NZBORA. Section 4 of the NZBORA states that no other statute shall be deemed invalid for the sole reason that the statute is inconsistent with any of the rights and freedoms contained in the NZBORA. This section is a clear statement by Parliament that other inconsistent legislation may trump provisions in the NZBORA. Accordingly, the courts will not invalidate s 228 of the CEA 2018 only because s 228 is inconsistent with any of the rights engaged in an electronic search context. The *generalis specialibus* maxim also favours the specific CEA 2018 legislation over the general NZBORA provisions.

To provide for greater privacy protection under the NZBORA, there are two recommendations. The first is to codify a right to privacy. Although s 28 states that a right not contained in the NZBORA does not preclude it from being recognised, a clear statutory provision for a privacy right would elevate the status and priority accorded to privacy. The second recommendation is to entrench the NZBORA to provide greater power for the courts to strike down legislation inconsistent with rights and freedoms. Both recommendations warrant their own rich discussions, so their merits and drawbacks will not be discussed in this article.

VI Conclusion

As put by the United States Supreme Court, for many people, the modern cell phone holds "'the privacies of life'".[161] With staggering amounts of personal information located on each device—some of which device owners would be highly uncomfortable sharing with anyone else—the ubiquity of electronic devices poses new legislative challenges. In particular, the law must grapple with balancing individual privacy interests with other rights, powers and obligations.

This article has explored the privacy interests and the competing interests engaged by s 228 of the CEA 2018, which permits warrantless searches of electronic devices at the border. It has analysed the interaction between the CEA 2018 and both the Privacy Act and the NZBORA, noting inconsistencies between the general statutes and the specific CEA 2018 legislation. While this article views the CEA 2018 as a good first attempt, it argues that

157 NZBORA, s 21.
158 Section 17.
159 Section 14.
160 Section 13.
161 *Riley v California*, above n 103, at 403.

Parliament has not legislated sufficient safeguards to protect privacy. Using analogies to physical search principles, this article has recommended a proportionality principle and restricting the permissible scope of electronic searches. Though drastic, this article has also built a case for repealing s 228 and requiring warrants for all electronic device searches at the border.