Public Interest Law Journal of New Zealand

(2022) 9 PILJNZ 25

ARTICLE

Still Waiting to Go Dark Nearly 30 Years On: The Privacy Implications of End-to-End Encryption (E2EE)

BENJAMIN CHRISTY*

The strongest type of communicative encryption, end-to-end encryption (E2EE), has been rolled out across most major messaging platforms, including as default on the largest provider, WhatsApp. The proliferation of this technology offers an unprecedented opportunity for ordinary citizens to radically protect the privacy of their communications with little effort. However, governments, law enforcement and intelligence agencies are fighting back with countervailing measures and laws aimed at protecting against what they see as an unjustified risk to public safety. This article charts the privacy–public safety debate with a focus on its relevance to a sound philosophical, legal and ethical position on E2EE for Aotearoa New Zealand's legal system. Drawing upon examples from the European Union, Australia, the United Kingdom and the United States, the article explores the relevant stakeholders, privacy interests, global approaches to E2EE and possible solutions to this debate. The article concludes that the best position is to support strong communicative privacy and E2EE while rejecting any encryption weakening technologies absent sufficient oversight. Ultimately, Aotearoa New Zealand should adopt a technologically and legally defensible position rather than enacting emotionally clouded emergency legislation in the wake of a crisis exacerbated by E2EE.

[*] BGlobalSt/LLB(Hons), Waipapa Taumata Rau—University of Auckland. This article is based on a research paper first written for a Privacy Law honours seminar course in 2021. The author is grateful for the profound wisdom and expertise imparted by Associate Professor Stephen Penk throughout that course. The author is further grateful to the countless editorial individuals whose feedback made this article possible.

I Fear Not: The Second Crypto-Wars are Here

It used to be commonplace for people to have private face-to-face conversations that were stored nowhere except for the interlocutor's memory. However, globalisation, technology and COVID-19 mean many conversations now occur through messaging technologies with complete recall and limited privacy protections. Messaging platforms have increasingly implemented the strongest form of communicative privacy protection, end-to-end encryption (E2EE), to combat this growth. While this development appears prima facie positive, below the surface bubbles a more sinister debate around the access that states should have to our private communications. E2EE brings this debate to the surface as it places our communications beyond the reach of the state and messaging providers. In response, nearly 30 years after the first Crypto-Wars, governments have reignited the moral panic of the risk posed to public safety by inaccessible communications, which they call "going dark". In short, privacy won the first Crypto-Wars and encryption was rolled out internationally. Nevertheless, can privacy really expect to win again in an age of terrorism and child sexual abuse material?

This article addresses the privacy implications of E2EE technologies available on numerous popular messaging platforms. It seeks to define, synthesise, and debate some of the most contentious privacy and public safety issues around the increased use of E2EE. The purpose of this is to provide a sound and rational philosophical, legal and ethical position that governments, like Aotearoa New Zealand's, should enshrine in law. The rapid development of E2EE technology and countervailing initiatives require decisive decision-making before Big Tech takes the reins at this global turning point. This article forms part of the vital public debate that we must have around such issues, before we are forced to address them by passing emotionally clouded emergency legislation in the wake of a horrific crisis—which we may or may not have avoided without E2EE. It is necessary to address the vast extra-legal chasm currently plaguing lawmakers and judiciaries on this issue.

Beginning with Part II, this article will explain the technological fundamentals of encryption and E2EE. Part III will explain how privacy rights are directly engaged and sets out the stakeholders involved in E2EE. Part IV will examine historical and current governmental approaches to E2EE and how they accord with privacy rights. Part V will explain the soundest privacy-affirming position that legislatures and courts should take. Finally, Part VI makes some overall recommendations based on this research.

II E2EE Explained

A *The technology*

E2EE protects data-in-transit between devices used for communication. It is not designed to, and does not, protect data-at-rest stored on a device. When a message is sent, it passes from the sender to the messaging provider's server, and then to the receiver. For standard SMS texts, the message travels along this route in a plaintext format—meaning it can be read and understood at any point if intercepted during transit. SMS thereby employs no encryption. Encryption is a process in which plaintext is converted into secret text (ciphertext) by running it through a mathematical algorithm with an encryption key. An encrypted message can only be intelligibly understood by those with the correct encryption key to convert the ciphertext back into intelligible plaintext.

In contrast to unencrypted SMS texts, messaging applications often use one of two encryption methods, point-to-point encryption (P2PE) or end-to-end encryption (E2EE). As its name suggests, P2PE means a message only exists as unintelligible ciphertext between communicative points—that is, between the sender and server, and between the server and receiver. However, the message is in completely intelligible plaintext for the sender, receiver, and at the messaging provider's server. The server often stores a plaintext copy of the message. The message can be converted into plaintext because the provider always stores a single symmetric encryption key for both encryption and decryption.

In contrast, E2EE means a message is in unintelligible ciphertext between communicative end points—it is unintelligible at all points between the sender and receiver. The message is completely unintelligible within the messaging provider's server, or if otherwise intercepted, as the provider does not have access to the encryption key to decrypt and read the plaintext message. This is achieved by using two separate but mathematically related asymmetric encryption keys: one for encryption and one for decryption. The server and sender can only access the public encryption key stored on the server. But only the receiver can access the private decryption key stored on the receiver's device. This demonstrates why E2EE is the most secure form of messaging, as it limits access to messages to the sender and intended receiver.

It is helpful to make one final observation about E2EE. Ultimately, the secrecy of E2EE messages relies on the secrecy of the private decryption key stored on the receiver's device. If this key is public or held by the provider, then any message can be decrypted, just like in P2PE. That encryption relies on the secrecy of an encryption key rather than the secrecy of the encrypting algorithm is a principle of fundamental importance to modern cryptography.[1] This Kerckhoffs' principle enables encryption algorithms to be publicly available for testing to fix vulnerabilities without compromising individual privacy maintained through one's secure unique keys.[2] However, even with algorithmic transparency and public testing, "security deficiencies may not be uncovered for years".[3]

B *How does E2EE support communicative privacy?*

Understanding E2EE's methodology further highlights how E2EE supports communicative privacy. E2EE provides four independent protections: confidentiality, integrity, authentication and non-repudiation.[4] Confidentiality is maintained by only allowing the sender and receiver to read the plaintext message. The message remains encrypted throughout the transfer process, removing any chance of alteration and maintaining the integrity of the message. E2EE also allows the sender and receiver to verify, independently of the messaging platform, that their devices are both the message's source and destination. This is done by ensuring their authentication codes match in-person or through another platform, such as the security code used by WhatsApp. Finally, this protection provides confidence that the sender was the only person who could have sent the message and so cannot repudiate sending it. All this is to say that, in its current form, E2EE primarily protects a communication's content and integrity and does not extend to protect communicative privacy interests beyond such content. These privacy interests

[1] Niels Ferguson, Bruce Schneier and Tadayoshi Kohno *Cryptography Engineering: Design Principles and Practical Applications* (Wiley Publishing, Indianapolis, 2010) at 24–25.

[2] At 24–25.

[3] At 13.

[4] Ben Lutkevich and Madelyn Bacon "end-to-end encryption (E2EE)" (June 2021) TechTarget <www.techtarget.com>.

become important when examining the other information governments can access beyond a message's content.

C *The usage*

E2EE is widely used. The leading global messaging application, WhatsApp (owned by Facebook/Meta), has end-to-end encrypted all private and group chats and calls since 2016.[5] That means that over 2 billion regular monthly users send over 100 billion E2EE messages daily.[6] New Zealand's largest messaging application, Facebook Messenger, currently offers opt-in E2EE in secret chats and is working towards implementing default E2EE.[7] Apple also offers E2EE for an estimated 1.3 billion iMessage users,[8] although iCloud backups—which are enabled by default—break this encryption unless manually disabled.[9] Other popular messaging apps, such as Viber (1 billion users), Line (700 million users), Telegram (200 million users) and Signal (not published), also offer default E2EE.[10] From this perspective, future trends indicate the increased introduction of E2EE as the technology grows better, cheaper and more necessary to implement.

III Communicative Privacy and the Spy Next Door

A *Communicative privacy*

Privacy, whether as an interest or a right, is typically not absolute but is balanced against other interests or rights. It is a right imbued with an internal qualifier: that of one's reasonable expectation. Despite the fact that privacy is a qualified right, the protection it provides is extremely important due to its function as a meta-right. According to the Austrian privacy lawyer Max Schrems, the protection of the right to privacy exists on two levels.[11] First, the right protects against a concrete breach of private data. Secondly, the protection of the right will be engaged to the extent that a person alters their behaviour when they feel they may be surveilled, even if constant surveillance of the person is impossible. The law is responsive to both of Schrems' levels. It regulates private data, not just to prevent its disclosure but also to protect our freedom of action. That is to say, privacy, while somewhat amorphous, is a vital meta-right.[12] It is through privacy that one can access and exercise other rights about which one cares more deeply. Privacy enables

[5] WhatsApp Help Center "Abut end-to-end encryption" <https://faq.whatsapp.com>.

[6] Brian Dean "WhatsApp 2022 User Statistics: How Many People Use WhatsApp?" (5 January 2022) Backlinko <www.backlinko.com>.

[7] Thomas Hinton "Leading social messenger apps, chat, and VOIP apps in New Zealand in 3rd quarter 2020" (February 2021) Statista <www.statista.com>; and Ruth Kricheli "Messenger Updates End-to-End Encrypted Chats with New Features" (13 August 2021) Messenger News <https://messengernews.fb.com>.

[8] Robert Triggs "Why iMessage is such a big deal: A guide for the rest of the world" (17 October 2022) Android Authority <www.androidauthority.com>.

[9] Chris Hoffman "Apple's iMessage Is Secure ... Unless You Have iCloud Enabled" (30 July 2021) How-To Geek <www.howtogeek.com>.

[10] Tess G "10 Most Secure Messaging Apps – The Best Platforms & Solutions" (8 March 2022) Stream <https://getstream.io>.

[11] Max Schrems "Why I sued Facebook over their data collection" (Internetdagarna 2019, Stockholm, 26 November 2019).

[12] Schrems, above n 11.

freedom of expression, thought and association; freedom from discrimination; the right against self-incrimination; freedom of the press; and the ability to preserve a private space.

Given privacy's vital status as a meta-right, we must turn to what privacy demands regarding messages. The term "communicative privacy" is suggested and used in this article to capture the multiplicity of privacy interests engaged in any communicative exchange. Communicative privacy is not just limited to the contents of communications but also includes the interlocutor's identity, associates, location, likes and dislikes, habits, and even sensitive health or financial data.

Communication, as the direct manifestation of our private thoughts, inherently contains a high expectation of privacy. One's private thoughts arguably remain the most private matter in this world. However, for humans as social creatures, thoughts are nothing but for their ability to be shared, refined and utilised to form communities. Since this is done through communication, communication is the closest, most authentic form of self-expression, second only to our private thoughts. As such, the contents of one's thoughts, in their expression as digital communications, should be protected by the highest degree of privacy preservable in the hyper-surveilled world in which we live.

While there is no absolute right to privacy, communicative privacy must fall at the stronger end of one's reasonable expectation. In a public setting, communications are not as readily observable as one's appearance or physical location which, for better or worse, are more easily subjected to surveillance. This is because communications can only be observed and surveilled when an individual has consciously exercised their choice to speak. Given this conscious choice, there would have to be a compelling reason to override the inherent expectation of privacy in relation to who the individual intended to be privy to such communications. This is especially the case in the context of law enforcement. For instance, where incriminating information can be obtained with minimal invasion to privacy, this should always be preferred to accessing communications between individuals not intended for use by law enforcement agencies.

In addition to strong reasonable privacy expectations for communications, privacy expectations can also be adjusted depending on how an individual exercises their choice to speak. This ability to adjust privacy expectations for in-person conversations provides a useful analogy for approaching digital communications. The privacy of in-person communications depends on factors such as the geographic location of communications and the proximity of speakers to others—factors obvious to all communicators. Conversations that previously would have happened exclusively in-person, can now occur through SMS or messaging applications. However, digital communications are still similar to real-life conversations in that their levels of privacy can be adjusted depending on the platform used. With a proliferation of available options, from email to SMS to AOL Instant Messenger to full-service social media platforms, individuals can somewhat customise their level of privacy. Despite being the fax machine of privacy standards, SMS is still globally popular, though it should be noted that billions have flocked to messaging apps, all encrypted to varying levels. E2EE has been employed across some of the most popular.

Analogising digital communication to in-person communication enables us to explore how different technological platforms create expectations of privacy. Being completely unencrypted, SMS is like a conversation in public held at a moderate volume. Not everyone will hear everything or understand it, but it would not be too difficult for anyone intent on following the conversation to do so. P2PE brings the conversation into a private location, like a living room. The conversation is mostly private, but there is little preventing other people in the house from eavesdropping or walking in to join the conversation. Finally, E2EE is akin to choosing a private location, speaking at a low volume and only to whom you intend to convey the message, all the while using a code or language only the speaker and listener can understand.

If a court were to look at the privacy right entailed by the latter in-person conversation, they would find a reasonably strong expectation of privacy. Using E2EE subjectively evinces an intention to preserve communicative privacy. As to the objective question of whether this expectation is reasonable, society would likely deem this preservation of privacy as reasonable, given its similarity to the private home analogy and the precautions taken in making the communication. If there was ever a strong case for a reasonable expectation of communicative in-person privacy, this would be it. This ultimately shows that of all the levels of communicative privacy, E2EE objectively demonstrates the strongest desire to assert privacy over a communicative instance.

Drawing this discussion together, it is clear that communicative privacy should be highly protected in the balance against other rights, as the privacy of communications are at the core of what privacy protects. On top of this, using a platform with E2EE provides the strongest possible assertion of such a right.

B *Governmental interests*

Governments rely on two countervailing interests to contest claims of communicative privacy. The first is the public's right to safety from threats to national security and serious crimes, especially child sexual abuse material (CSAM), murder and drug offences. The second is the corollary duty of law enforcement and intelligence services to protect the public.

Governments frame the E2EE debate around the public safety interest. E2EE removes the ability of law enforcement to access the plaintext of encrypted communications, even if they can compel providers to release the ciphertext. Without the private decryption key, any information contained in the plaintext, be it CSAM or a planned terrorist attack, is unintelligible. This lack of access to communications, which law enforcement and intelligence agencies term "going dark", places more of their formerly available evidentiary materials beyond easy access.[13] As a result, these agencies worry about their ability to prevent terrorism and solve crimes.

E2EE also reduces the ability of intelligence agencies to conduct mass surveillance of communications, a practice more possible with unencrypted or P2PE communications. In contrast, the widespread use of E2EE necessitates more intensive, targeted surveillance efforts.

These state interests combine to form a seemingly palatable argument against E2EE in the name of protecting children and the wider public. In response to privacy concerns, the classic response of "if you have nothing to hide, you have nothing to fear" comes to mind. However, there is good reason to doubt the validity of these claimed government interests and to examine whether the statistics support the state's concerns.

While it can be acknowledged that the widespread usage of E2EE may compromise a government interest in public safety, governments have been disingenuous when promoting this line of argument. First, the statistics, at least thus far, do not paint a clear picture of the supposedly lawless society that law enforcement and the intelligence sector

[13] James B Comey, Director of the Federal Bureau of Investigation "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" (speech to the Brookings Institution, Washington DC, 16 October 2014).

fear. In Aotearoa New Zealand, to the best of this author's knowledge, there are no publicly available statistics about the extent of this problem. A recent study in the Netherlands also found no statistical difference in the prosecution of E2EE and non-E2EE evidence cases.[14] However, the most concerning example would be a case from the data-at-rest field. In 2017, the United States Federal Bureau of Investigation (FBI) routinely claimed, including during sworn congressional testimony, that it could not access data on 7,775 devices.[15] It later eventuated that an apparent "programming error" by the FBI meant its numbers were severely overestimated, with the actual number closer to 1,200 devices.[16] Some scholars have suggested the FBI overexaggerated their difficulties with encrypted communications in high-profile court cases when they could easily have sought technical solutions—arguably misleading the court about the true extent of the challenges posed by E2EE.[17] This example severely undermines law enforcement's credibility, transparency, trustworthiness and competence in this space, even in providing sworn advice to lawmakers. We must be highly sceptical of law enforcement and intelligence agencies' true motives and the assertions they make when balancing public safety with public privacy.

Secondly, politicians and enforcement executives appear to enjoy the political capital and investments gained by politically grandstanding on this issue. Calls to break E2EE often focus on sympathetic victims, such as protecting children from CSAM.[18] While a laudable goal, privacy advocates again must be wary of the true intentions of government and law enforcement. While breaking E2EE may well help with CSAM investigations, it may equally help with mass surveillance or solving drug crimes, issues for which a privacy-conscious public may be less willing to risk their rights.

Additionally, various governments have stressed that they are simply trying to encourage messaging providers to comply with their duty to enforce their terms of service.[19] But when has one ever heard Parliament debate how to help large companies enforce their own policies? This appears to be a convenient subterfuge about an issue the government cares very little about.

There appears to be a trend of politicians finding it hard to comprehend technical realities and instead hiding behind positive but baseless talking points. In 2017, then United States Deputy Attorney-General Rod Rosenstein supported the idea of "responsible encryption", an idea that spoke volumes to the access that law enforcement should constitutionally have, yet which failed to deliver any technically feasible solutions without breaking encryption.[20] Former United Kingdom Home Secretary Sajid Javid claimed the messaging app Telegram was a "mouthpiece for terror" without actually offering any idea

[14] Pieter Hartel and Rolf van Wegberg "Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases" (15 April 2021) arXiv <arXiv:2104.06444v1> at 7.

[15] Devlin Barrett "FBI repeatedly overstated encryption threat figures to Congress, public" *The Washington Post* (online ed, Washington DC, 22 May 2018).

[16] Barrett, above n 15.

[17] Susan Landau "Revelations on the FBI's Unlocking of the San Bernardino iPhone: Maybe the Future Isn't Going Dark After All" (30 March 2018) Lawfare <www.lawfareblog.com>.

[18] WePROTECT Global Alliance *Global Threat Assessment 2021: Working together to end the sexual abuse of children online* (2021) at 33–34.

[19] Andrew Little "International statement – End-to-end encryption and public safety" (press release, 12 October 2020).

[20] Rod J Rosenstein, United States Deputy Attorney-General "Remarks on Encryption" (speech to the United States Naval Academy, Annapolis, 10 October 2017).

on what he intended to do about it.[21] Javid's predecessor, Amber Rudd, claimed she did not need to understand encryption to know it "helps criminals", but again could not elaborate on how or why such technologies assisted criminals or what privacy interests were at stake.[22]

In sum, governments have a legitimate interest in public safety and the corollary duty to protect the public. No one would claim that the prevention of serious crimes such as CSAM and terror threats are unworthy causes. However, it is necessary to challenge state claims on two fundamental points. First, it may not be worth or even necessary to risk everyone's private E2EE communications to combat these threats. Secondly, governments may lack credibility when making claims about the need to protect the public.

C *Interests of surveillance intermediaries*

Finally, we cannot overlook the interests of vital third parties: the messaging service providers themselves. Alan Z Rozenshtein terms these surveillance intermediaries, "large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance".[23] Rozenshtein further notes that while these intermediaries are bound by legislation and court orders, they exercise broad discretion in how they assess and respond to requests from the state to release private user data.[24] They may choose the speed at which to comply, the extent of the information released, and whether they challenge an order on procedural or substantive grounds. However, it must be noted that encryption, especially E2EE, is just another tool for messaging providers to control how and whether they comply with such requests.

It should also be noted that providers need not, and indeed do not, take a uniform approach to requests. For example, Apple took the FBI to court over a request to help provide access to data-at-rest on a password-protected iPhone.[25] In direct contrast to this, in 2017, Blackberry's CEO committed to the position of attempting to break their own encryption if court-ordered wiretaps required it of them.[26] However, Blackberry's position is seemingly unique in this field, and there has been an appreciable rise in litigation promoting encryption by tech companies, especially following Edward Snowden's 2013 revelations of global mass surveillance.[27]

Messaging providers have only assumed responsibility as surveillance intermediaries because of the widespread popularity of their products, rather than through a deliberative process that elected the most preferable actor to assume this role. Yet from a technological perspective, it would seem practically impossible to assign this role to anyone other than the provider. Tech companies play a significant role in the extent to which privacy is protected and how it is balanced with governmental public safety interests. What each surveillance intermediary chooses to do will ultimately depend on

[21] Victoria Ward, Steven Swinford and Dominic Nicholls "Telegram app is 'mouthpiece' for terror, Sajid Javid says as jihadi admits encouraging attack on Prince George" *The Daily Telegraph* (online ed, London, 31 May 2019).

[22] Brian Wheeler "Amber Rudd accuses tech giants of 'sneering' at politicians" (2 October 2017) BBC <www.bbc.com>.

[23] Alan Z Rozenshtein "Surveillance Intermediaries" (2018) 70 Stan L Rev 99 at 105.

[24] At 122–125 and 138–139.

[25] Tim Cook "A Message to Our Customers" (press release, 16 February 2016).

[26] Thomas Brewster "BlackBerry CEO: We'll Try To Break Our Own Encryption If Feds Demand It" *Forbes* (online ed, Jersey City, 25 October 2017).

[27] Daphna Renan "The Fourth Amendment as Administrative Governance" (2016) 68 Stan L Rev 1039 at 1127.

profitability, current events, technical structural realities, business models and the interests of corporate and individual users.[28] However, the effects of these decisions will result in wide-ranging consequences for privacy and public safety. They may even go beyond the law. Shockingly, the United States telecommunications conglomerate AT&T and the National Security Agency (NSA) operated an internet surveillance platform from 2001 to 2008 without legal authorisation.[29] This example further proves the necessity of clear legislative oversight that genuinely aims to prevent privacy interests from being compromised.

IV Taking a Position: Analysing Global Approaches

Having comprehensively assessed the competing rights and stakeholders at issue, this article now turns to some of the most popular solutions to maintaining the balance between privacy and public safety concerns. This Part also addresses some of the fundamental shortcomings of many of these suggestions and illuminates the values that are really at stake.

A *Backdoors*

The most radical challenge to E2EE and its protection of message content privacy is the implementation of features known as "backdoors". Backdoors are deliberately designed to bypass encryption and subsequently access communications without a user's authorisation.[30] While almost all of the proposals discussed in this section are varying forms of backdoor technologies, this initial discussion focuses more generally on the compellability and desirability of messaging providers to institute backdoors.

Let us begin with the mechanics of a simple backdoor proposal. The United Kingdom's Government Communications Headquarters (GCHQ) has suggested a "ghost protocol" backdoor, whereby law enforcement and intelligence agencies would be added as invisible participants to E2EE private and group chats.[31] Such a proposal enables access to a communication's contents, which interlocutors are unaware of, and would bypass encryption as the government is directly party to the conversation. This would theoretically open up every conversation to this type of snooping, thereby removing the authentication privacy guarantee of participant identities that E2EE provides. The issue is then whether messaging companies can, or should, be compelled to build or implement such backdoors.

In respect of this question, Australia's legislative regime is arguably the least privacy-respecting, anti-E2EE and pro-law enforcement of any Western democracy. The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA) provides sweeping executive powers to combat encryption.[32] TOLA introduces

[28] "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance" (2018) 131 Harv L Rev 1722 at 1730–1736.

[29] Julia Angwin and others "AT&T Helped U.S. Spy on Internet on a Vast Scale" *The New York Times* (online ed, New York, 15 August 2015).

[30] Alec Muffett "What do we mean by a 'backdoor' in End-To-End Encrypted Messengers or Secure Messengers?" (1 March 2021) Dropsafe <https://alecmuffett.com>.

[31] Natasha Lomas "Apple, Google, Microsoft, WhatsApp sign open letter condemning GCHQ proposal to listen in on encrypted chats" (30 May 2019) TechCrunch <https://techcrunch.com>.

[32] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) [TOLA].

three types of notices that can be issued to enable federal or state law enforcement and Australia's national security agency, ASIO, to gain access to encrypted information for which they would otherwise have required express permission to access—in the form of a warrant, statutory power, or court order. First, a Technical Assistance Request (TAR) is a voluntary request for a designated communication provider (DCP) to use decryption or other access capability they already possess.[33] Secondly, a Technical Assistance Notice (TAN) acts the same way as a TAR, but is compulsory.[34] Thirdly, a Technical Capability Notice (TCN) is a compulsory notice that requires DCPs to build new capabilities to enable future compliance with TARs and TANs.[35] It should also be noted that the broad definition of a DCP applies extraterritorially and captures all messaging applications, so long as "one or more end-users [is] in Australia".[36]

Worryingly, all requests and notices are issued through a secret executive branch discretionary process that possesses no judicial oversight.[37] TARs and TANs are issuable by the requesting agencies' chief officer, are not subject to judicial oversight and can only be investigated after the fact by the Commonwealth Police Ombudsman or the Inspector-General of Intelligence.[38] For TCNs, which could compel messaging providers to build backdoors, only the Attorney-General and Minister of Communication need to jointly approve a notice.[39] In all cases, issuers must satisfy the requirement that assistance would be "reasonable and proportionate", and that compliance would be "practicable and technically feasible" and consider other interests, including legitimate expectations of privacy.[40]

As of August 2020, the only notices and requests issued under the Act are TARs, suggesting that companies are choosing to voluntarily comply rather than be saddled with compulsory obligations.[41] ASIO has issued "fewer than 20", Federal Police only eight and the New South Wales State Police 13 of these notices.[42] It should also be noted that corporate non-compliance with any notice is subject to an AUD $10 million civil penalty.[43]

The Australian approach raises numerous concerns about the ability of E2EE to protect communicative privacy. Primarily, the approach lacks sufficient independent judicial and technical oversight. It is worrying that TCNs possess such extensive powers in compelling the creation of backdoors into E2EE. Executive officials are naturally more likely to exercise discretion in favour of investigations or for the purposes of being "tough on crime", especially when there is limited rights-affirming oversight. As part of the executive, even if officials consider privacy, they are ill-equipped to fully appreciate privacy interests and adopt a reasonable proportionality approach—something regularly delegated to the courts. Likewise, executive officers and even the courts themselves are unlikely to

[33] Section 317G.

[34] Section 317L.

[35] Section 317T.

[36] Section 317C.

[37] Stilgherrian "The Encryption Debate in Australia: 2021 Update" (31 March 2021) Carnegie Endowment for International Peace <https://carnegieendowment.org>.

[38] See TOLA, s 317G for issuance and s 317L; and see ss 317HAB, 317 MAA and 317MAB for initial notification of the Ombudsman and Inspector-General and complaints process.

[39] Section 317TAAA.

[40] Sections 317JAA, 317P and 317WA(7).

[41] Parliamentary Joint Committee on Intelligence and Security *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Official Committee Hansard, 7 August 2020) at 12, 13 and 26.

[42] At 12, 13 and 26.

[43] TOLA, s 317ZB.

appreciate the technical realities and privacy risks inherent in adapting E2EE technologies. Consequently, any powers that have the potential to fundamentally wipe out E2EE's privacy protections must be subject to vigorous independent rights and technical screening. It would be reasonable to consider the United Kingdom's approach in similar legislation—requiring TCNs to have the approval of the Secretary of State *and* independent judicial authorisation—as a baseline.[44]

Privacy would ultimately be better protected if the executive power to compel backdoors was never enshrined in legislation. A better approach would be for Parliament, if ever required, to pass affirmative legislation, through normal channels, of the proposed contents of TCNs. Parliamentary checks provide greater oversight and public transparency for notices that have a profound impact on constituents' rights. To counter any arguments that legislating TCNs would be too burdensome, it should be noted that no such order has yet been made in Australia and that, given their privacy implications, TCNs should be made as a means of last resort. While, ideally, no TCNs would ever need to be issued, the use of affirmative legislation would at least provide the ability to do so while supporting communicative privacy. In Parliamentary supremacy systems such as our own, forcing the explicit legislation of backdoors that breach privacy rights is the only way for the public to hold the government to account at the ballot box.

B *Key escrow*

The simplicity of key escrow proposals is what makes them most threatening to the privacy protections provided by E2EE. As highlighted earlier, the ability to keep one's private decryption key secret is foundational to the security of E2EE. Key escrow exploits this necessity by storing a copy of one's private decryption key escrowed with the provider or a third party.[45] While this means that a provider, with or without a third party, could decrypt messages, proponents argue this does not turn E2EE into P2PE. The private key database would not be routinely used for decryption but only in accordance with the escrow policy or as compelled by law. One famous example is the now defunct Clipper Chip proposed by the NSA in 1993.[46] The Clipper Chip was a physical device to be installed in newly manufactured phones and would transmit a decryption key to be held by the government in escrow should they ever need to intercept cell phone transmissions.[47] Modern day examples suggest software solutions where one's private decryption key is stored in escrow by the provider or a government department.

Key escrow proposals threaten the privacy of communications due to the security issues related to maintaining a mass private key database. Such a database, conveniently compiled for police and intelligence agency use, would prove irresistible to cyber criminals and even foreign governments. Whether providers should invest in strong enough security to guarantee against hacking and whether installing such security is even possible is uncertain.[48] The main issue is that once aware that such valuable keys are stored in a

[44] Investigatory Powers Act 2016 (UK), s 253.

[45] Bill Buchanan "Keys Under The Mat: NOBUS, Key Escrow, or a Crumple Zone?" (12 August 2018) Medium <https://medium.com>.

[46] The White House "Statement by the Press Secretary" (press release, 16 April 1993).

[47] Matthias Schulze "Clipper Meets Apple vs FBI—A Comparison of the Cryptography Discourses from 1993 and 2016" (2017) 5(1) Media Communications 54 at 55.

[48] Matthew Green "A few thoughts on Ray Ozzie's 'Clear' Proposal" (26 April 2018) Cryptography Engineering <https://blog.cryptographyengineering.com>.

certain location, bad actors can target them, much like how we know that a bank keeps money or a hospital keeps health records.

The problem can be illustrated by an example in the banking sector. Hackers have managed to gain international SWIFT credentials and pose as legitimate bank employees to steal millions of dollars internationally.[49] These credentials might as well be anyone's private decryption messaging key, which could be used to uncover messages or pose as an individual for future messaging. The difference between a key database and SWIFT, as well as the aforementioned bank and hospital examples, is that banks and hospitals need to have money and patient records to provide their services. Privacy and security risks need to be accepted for these vital services to endure. In contrast, E2EE messaging apps function perfectly well and are more secure without the key vault. In this case, creating a private key vault would be a *choice* which would massively increase the privacy risk for a function that is not operationally necessary.

There may come a time in the future when the security of a key vault can be guaranteed, but for now, the technology risks ending up like the Titanic: the unhackable vault that was hacked. Under these circumstances, it must be accepted that the onus of proving that privacy will be protected through an unbreakable system lies on those seeking to create that system. In other words, "if your proposal fundamentally relies on a secure lock that nobody can ever break, then it's on you to show me how to build that lock".[50]

C *Content monitoring: Client-side scanning (CSS)*

Content monitoring solutions are one of the main solutions proposed by surveillance intermediaries. These solutions aim to find CSAM or terrorist content by determining when such material is posted, all without breaking encryption.

Client-side scanning (CSS) screens content for certain material before it is encrypted and transmitted to the recipient.[51] The screening could be for any unlawful material, from key words or files to photos and videos.[52] Any material could then be flagged to the provider, law enforcement, sender or any combination thereof—though the most obvious action would be to pass this information on to the relevant government investigative authority.

One example of CSS includes image screening conducted through perceptual hashing (a unique photo fingerprint) or machine learning.[53] In its iOS 15 update, Apple was set to implement such a scanning tool to scan for CSAM in any photographs securely sent to iCloud backups.[54] However, concerns by prominent cryptographers and computer scientists stalled this and iOS 15 was eventually released without this feature.[55] While development is rumoured to be going ahead, Apple has remained silent on the software's

[49] Tom Bergin and Jim Finkle "Exclusive: SWIFT confirms new cyber thefts, hacking tactics" *Reuters* (online ed, London, 14 December 2016).

[50] Matthew Green, above n 48.

[51] Erica Portnoy "Why Adding Client-Side Scanning Breaks End-To-End Encryption" (1 November 2019) Electronic Frontier Foundation <www.eff.org>.

[52] Portnoy, above n 51.

[53] Thomas Claburn "Client-side content scanning is an unworkable, insecure disaster for democracy" (15 October 2021) The Register <www.theregister.com>.

[54] Chance Miller "Apple delays rollout of CSAM detection system and child safety features" (3 September 2021) 9To5Mac <https://9to5mac.com>.

[55] Miller, above n 54.

development and removed all mentions of it from their website in December 2021.[56] Alongside the numerous security vulnerabilities posed by this method, experts contend that CSS generates false positives, may rely on proprietary technologies that limit auditing, and is capable of being subverted and evaded.[57]

This use of CSS has the potential to wreak havoc on communicative privacy. Scanning every communication effectively subverts E2EE and would be akin to mass surveillance. While the intention of CSS is that providers and then law enforcement would be warned of any unlawful material, everyone's privacy is being compromised in this circumstance, with a very real chance for private communications to be wrongfully revealed due to false positives. It is no wonder then that one website has dubbed CSS "an unworkable, insecure disaster for democracy".[58]

D *Trojan spyware: An end point workaround*

One of the more unique approaches available that does not break E2EE is Trojan spyware, also known as end point workarounds. E2EE ensures that communications exist as unintelligible ciphertext during transmission, but they are intelligible to the sender and receiver. Trojan spyware exploits this by reading the plaintext off the sender or receivers' device at the communication end points, existing outside of the transmission process and encrypted system.[59] It is a clever solution and, as one former GCHQ director has admitted, the easiest way to bypass E2EE.[60] The installation of Trojan spyware may require physical access to the device, a security vulnerability in the device, or the internet or software provider's permission.

Using Trojan spyware is a technique favoured by the German government. During the first Crypto-Wars, Germany adopted a policy preventing the banning of encryption but affirmed that "[t]he spread of strong encryption methods must not undermine the legal powers of law enforcement and security authorities to monitor telecommunications".[61] To remain compliant with this stance in the E2EE era, Germany passed a law in June 2017 allowing Federal Police to install Staatstrojaner, a Trojan spyware, without notice on suspects' phones for low and higher-level criminal and terrorist investigations.[62] Opponents of this law noted these changes were passed in an omnibus bill with other uncontroversial criminal procedural changes to hide their true effect.[63] In 2021, the

[56] Joe Rossignol "Apple Remains Silent About Plans to Detect Known CSAM Stored in iCloud Photos" (13 August 2022) MacRumors <www.macrumors.com>.

[57] Hal Abelson and others "Bugs in our Pockets: The Risks of Client-Side Scanning" (2021) arXiv <arXiv:2110.07450v1> at 8, 11, 13, 24 and 28.

[58] Claburn, above n 53.

[59] Kapersky "What is a Trojan horse and what damage can it do?" <www.kaspersky.com>.

[60] Interview with Robert Hannigan, Former GCHQ Director (Today, BBC Radio 4, 10 July 2017).

[61] *Eckwertepapier der Bundesregierung zur Kryptopolitik: Eckpunkte der deutschen Kryptopolitik* (2 June 1999) at 3 (translation: *Key Issues Paper of the Federal Government on Crypto Policy: Cornerstones of German Crypto Policy*). The quote is originally in German and has been translated into English by the author using the online translator, DeepL. The author takes responsibility for any inaccuracies in the translation.

[62] Strafprozeßordnung 1987, § 100a (translation: German Code of Criminal Procedure) as amended by Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens 2017, art 3 (translation: Act to make Criminal Proceedings more effective and practicable).

[63] Andre Meister "Staatstrojaner: Bundestag hat das krasseste Überwachungsgesetz der Legislaturperiode beschlossen" (19 June 2017) Netzpolitik <https://netzpolitik.org> (translation: "Bundestag passed the most blatant surveillance law of the legislative period").

German Bundestag extended these powers to Germany's 16 secret services and allowed retrospective access to messages that were made in the period after a wiretap warrant was granted but before it was implemented.[64] Both of these laws are the subject of ongoing Federal Constitutional Court proceedings on privacy grounds.[65] Also in 2021, the Bundestag attempted to radically extend the police's powers by allowing pre-emptive searches and compelling provider assistance in installing Trojan software.[66] Thankfully, the Bundesrat, German Federal Council, withheld consent, thereby preventing this legislation from taking effect.[67]

On one view, Trojan spyware should be the most favoured technique, seeing as it does not weaken E2EE due to its operating beyond the bounds of encryption. However, while not explicitly breaking that encryption, it does still effectively circumvent it by providing access to the private contents of communications. Nevertheless, the key theoretical distinction between Trojan spyware and other solutions is that the communication's contents are obtained without requiring others to compromise their privacy when using E2EE software. Trojan spyware can provide a targeted and specific approach to obtain the communicative contents only for those under investigation.

Unfortunately, the technical reality suggests that methods of installing Trojan spyware could still be utilised to compromise the security of all E2EE users. Most concerning are approaches, like Germany's 2021 proposal,[68] that suggest permitting the use of Trojan spyware in a widespread or pre-emptive manner. Law enforcement and intelligence agencies would pre-emptively install the software to check for unlawful material or store the communications that would be retrospectively accessed upon the granting of a court order. In such circumstances, there are clear privacy fears of function creep and mass surveillance. Notification of individuals being wiretapped is surely counterintuitive and not required, even for current standards of unencrypted phone wiretapping. However, as noted earlier, the subjective assertion of one's privacy expectation is higher when using an E2EE platform—individuals should generally be able to rely on the privacy afforded by E2EE. Widespread use or even targeted use of Trojan spyware would render apparent privacy protections utterly illusory. Beyond the contents of communications, there is still a loss of privacy in Schrems' terms, as individuals modify their behaviour in the fear that E2EE provides insufficient anti-surveillance protections, even if widespread surveillance is not occurring.

The only way to counter the above assertions would be to carefully regulate and use Trojan spyware only after specific independent judicial authorisation was made that

[64] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 – Gesetz – G 10) 2001, § 2(1a), 9 and 11(1a) (translation: Act on Restrictions on the Secrecy of Mail, Post and Telecommunications) as amended by Gesetz zur Anpassung des Verfassungsschutzrechts 2021, art 5 (translation: Act to Amend the Consitution Protection Law).

[65] Pia Stenner "G-10 Gesetz: FDP-Abgeordnete legen Verfassungsbeschwerde gegen Staatstrojaner ein" (15 July 2021) Netzpolitik <https://netzpolitik.org> (translation: "G-10 Act: FDP MPs file constitutional complaints against state Trojans").

[66] Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei 2021 (Drucksache 19/26541) (translation: Bill to Modernise the Legal Bases of the Federal Police). For the bill as passed by the Bundestag and presented for Bundesrat approval, see Bundesrat *Gesetzesbeschluss des Deutschen Bundestages* (Drucksache 515/21, 11 June 2021) (translation: *Legislative Resolution of the German Federal Parliament*).

[67] Bundesrat *Beschluss des Bundesrates* (Drucksache 515/21, 25 June 2021) (translation: *Decision of the German Federal Council*).

[68] Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei 2021, above n 66.

weighed privacy and the merits of other evidence in the case. Only after this should courts then issue prospective wiretap warrants akin to those currently used for non-encrypted voice communications. Trojan spyware is then downloaded onto the device of a target who, due to reasonable evidence of a specified crime, has an objectively diminished expectation of privacy.

While the benefits of this scenario sound positive and cannot be downplayed, the effectiveness of Trojan software may be limited, especially when considering the presence of anti-virus providers and the access required to download Trojan software. Furthermore, it must be noted that Trojan spyware still fundamentally enables access to the contents of private communications, thereby impacting consumer trust in E2EE software.

So far, end point workarounds seem to offer the most privacy-affirming solution by not explicitly breaking E2EE. Nevertheless, there are still real risks involved, especially if these workarounds continue to be used pre-emptively or on a mass surveillance level. However, this solution provides hope that in the event there are extremely narrow grounds, judicial safeguards and technical buy-in, it is possible to balance both privacy and public safety considerations in Western democracies.

E *The problem that isn't: Technical incapacity*

From the numerous proposals above, it is clear that the privacy argument often seems to be decided on the basis of whether the proposal is technologically sound. However, while these problems do exist and must be accounted for, they mask a deeper privacy issue. The presence of this issue is highlighted when considering what would happen if all proposals were suddenly without technological limitations, operating at their logical extremes. For example, if key escrow databases were 100 per cent unhackable, would the public then unreservedly accept these systems in the name of public safety? This author hazards not.

The real problem is that technological incapacity distracts privacy advocates from the heart of the issue: keeping conversations private and uninfluenced by the fear or undue influence governments may exert. Returning to Schrems' definition, we are unfree in that we lack privacy to the extent we change our behaviours for fear of being surveilled, even if it is impossible to monitor everyone's messages at once. The issue is therefore properly conceptualised as being about the relative levels of public trust in, and oversight of, government agencies and messaging companies. It is about what a reasonable sense of communicative privacy demands and to what extent non-interlocutors should have access to our private lives in a free and democratic society. The conversation can be reframed to look at what privacy protections we must have and how the law can then safeguard this, bearing in mind technological capabilities.

F *The authoritarian problem: Human rights and journalistic protections*

We have now reached the point where one may believe that, despite privacy concerns, a proposal with sufficient judicial safeguards could be implemented. This suggestion sounds especially plausible in a country like Aotearoa New Zealand, which generally has a strong respect for democracy and the rule of law. However, E2EE platforms are global, and so what is good enough for Aotearoa New Zealand must be good enough for everyone else. That is, even if we trust our government to not tyrannically obliterate privacy or remove judicial redress, there is no guarantee that we can trust all foreign powers to do the same.

By working with, or compelling, E2EE platforms to provide backdoors, escrow keys or install spyware, we are effectively setting a precedent for brutally oppressive regimes.

If we utilise CSS to monitor content for CSAM, nothing stops others from monitoring for content that discriminates against minorities and cracks down on challenges to government. In countries where being LGBTQ+ or having certain religious affiliations are criminal, privacy acts as a meta-right to protect such individuals from persecution. In a similar vein, it also protects journalists and their sources from persecution and their right to freedom of speech. Even a minimal compromise to E2EE puts the human rights of every one of these individuals at risk. China is a prime example of this, having blocked WhatsApp in 2017, just one year after it implemented E2EE.[69] It is also surely not a coincidence that none of the popular Chinese messaging applications (WeChat and QQ) have E2EE capabilities.[70]

All in all, democracies must pause to consider the protection of international human rights and journalists before rushing to implement solutions. Democratic states must ask themselves if it is truly worth catching a drug dealer in Aotearoa New Zealand only to know that the same technology helps perpetuate genocide overseas.

V Affirming the Absolute: Re-enshrining Communicative Privacy

In this Part, the article will draw from the aforementioned solutions to argue for a strong re-enshrining of communicative privacy in relation to E2EE. It will then propose the soundest privacy-affirming position that legislatures and courts, especially those in Aotearoa New Zealand, should take.

A *What is at stake: A case for absolutism*

We begin by recalling that privacy is not an absolute right and is balanced with other rights to preserve only one's reasonable expectation therein. The right must be informed more generally by the state's legitimate interest in surveillance and recording evidence of criminal activities to protect public safety. In this vein, invocation of the right to privacy also raises the question of whether alternative evidentiary material or access options would be less intrusive.

The technological realities of E2EE and the necessity of using messaging platforms fundamentally alters this equation. The problem is that every proposal for facilitating state interests over an individual's privacy right practically endangers everyone's privacy. Every time a provider or law enforcement agency seeks to compromise their system and release the contents of a message, the privacy of everyone is at risk. The privacy rights of the collective are being balanced against accessing evidence related to an individual criminal. However, this is not a balance, because the alternative is *no one* being able to assert a reasonable expectation of privacy. This is wholly unacceptable in a Western democracy.

The current state of E2EE technology makes clear that absolutist privacy is the only tenable position. States can and must affirmatively protect E2EE to preserve communicative privacy. The following sections explore this limited absolutism approach to E2EE communicative privacy and whether it is as harsh as it may sound.

[69] Keith Bradsher "China Blocks WhatsApp, Broadening Online Censorship" *The New York Times* (online ed, Shanghai, 25 September 2017).

[70] Shannon Liao "Over 300 million Chinese private messages were left exposed online" (5 March 2019) The Verge <www.theverge.com>.

B *The Dutch lesson*

No government has enshrined as strong a policy for supporting E2EE as the Netherlands. In January 2016, the Dutch government released an official statement signed by the Minister of Security and Justice, and the Minister of Economic Affairs, with the consent of the Dutch General Intelligence and Security Service and the Dutch National Counter Terrorism Coordinator.[71] This statement acknowledged there were no current possibilities to "weaken encryption products without compromising the security of digital systems" and stressed the importance of security "for supporting the protection of citizens' privacy".[72] It concluded by affirming that it was therefore "not desirable" to restrict any encryption and would "propagate this conclusion, and the arguments that underlie it, internationally".[73] This statement was upheld by the House of Representatives with a call for the government to advocate for it in the European Union and internationally.[74]

This position is a perfect reflection of the realities of privacy this article has already explored and shows how this position can be taken officially. It formally acknowledges that there is no compromise proposal that does not limit privacy and so implicitly affirms an absolute right to privacy. While this may seem radically out of step with other solutions proposed, it actually appears to have caused little harm. As mentioned above, a recent study found no difference between the conviction rate of Dutch offenders who used E2EE and those who did not.[75]

Unfortunately, despite the official Dutch position remaining as it is, there has been some limited backsliding. Dutch police and intelligence are now lawfully permitted to use any software or hardware vulnerabilities or glitches they uncover or purchase to get around E2EE.[76] However, this has limited use because every time a flaw is exploited, it must be reported to the manufacturer unless an independent court, taking into account privacy concerns, approves that the vulnerability may be left unfixed for a specified period.[77] While any subversion of E2EE is not ideal from a privacy perspective, Dutch reporting requirements mean these vulnerabilities will eventually be patched. The Dutch approach certainly prevents widespread mass surveillance. In addition to this, the time and expense of using exploits severely limits their usage to only the most necessary and severe cases of criminal wrongdoing. Consequently, the Dutch position still remains the strongest position on E2EE, with a rights-respecting way provided for when workarounds are needed.

[71] Ministers van Veiligheid en Justitie en van Economische Zaken "Kabinetsstandpunt encryptie" (Tweede Kamer der Staten-Generaal, 26643/383, 4 January 2016) (translated letter: Matthijs R Koot (translator) "Full translation of the Dutch government's statement on encryption" (31 October 2016) Matthijs R Koot's Notebook <https://blog.cyberwar.nl>).

[72] Koot, above n 71.

[73] Koot, above n 71.

[74] Kees Verhoeven and Roberta Francina Astrid Oosenbrug "Verwerking en bescherming persoonsgegevens: Motie Van De Leden Verhoeven En Oosenbrug" (Tweede Kamer den Staten-General, 32761/105, 2016) (translation: Processing and protection of personal data: Motion by Members Verhoeven and Oosenbrug).

[75] Hartel and Wegberg, above n 14, at 7.

[76] Tina Amirtha "Dutch police get OK to exploit zero-days: So will that just mean more surveillance?" (6 December 2016) ZDNet <www.zdnet.com>.

[77] Amirtha, above n 76.

C *Caught in the crosshairs: Law-abiding individuals*

It is important to note that all the solutions proposed to bypass E2EE are inherently futile in gaining evidence on experienced criminals, instead resulting in much higher costs to the communicative privacy of law-abiding civilians. Hardened criminals and crime groups will still continue as they have long before E2EE. For example, al-Qaeda has encrypted their communications through their own software, Secrets of the Mujahideen, since 2007.[78] Similarly, following Snowden's revelations in 2013, ISIL created a new encryption tool that same year.[79] Of law enforcement's targets, the only individuals really caught by weakened E2EE are relatively careless criminals, with the communicative privacy of the law-abiding public being collateral damage. If only careless criminals are caught because they used messages that are now discoverable, then it is highly likely they would have left other discoverable and admissible evidence elsewhere that is not in the form of E2EE encrypted messages. As a result, those states that claim cracking E2EE will assist in finding criminals are not meaningfully impacted by whether encryption exists. Despite this, the privacy impact will be felt by all law-abiding individuals.

To explain this, we turn to a readily understandable example. Currently, a warrant may be obtained for covert surveillance of a house, including audio of suspects and their mobile phone calls. The difference is that E2EE technology dictates that in order to surveil one house or one phone call, agencies would have to be able to, and may need to, surveil them all. With any of the proposed solutions to bypassing E2EE, there is little ability to reject a dragnet search of every individual who may be participating in unlawful activities. Next, the government may be knocking down walls because they hide private criminal meetings, or impounding cars because they allow criminals to make getaway attempts from police. These examples are obviously ludicrous, but a similar logic seems to apply. We must accept, respect and uphold the rights of law-abiding citizens in a democracy, even if it means future criminals benefit from those rights too. The only alternative to this is authoritarianism.

D *Determining the need: Where's the data?*

Another argument that supports continued E2EE privacy is that there is insufficient evidence of the need to decrypt messages to solve crimes. WhatsApp has had E2EE since 2016,[80] and encryption technology was rolled out internationally at the end of the first Crypto-Wars in the late 90s.[81] However, law enforcement and intelligence agencies cannot point to any major trends of E2EE preventing them from doing their jobs or obtaining convictions. The best data available is from a questionnaire conducted of EU Justice Ministers by the Council of the European Union in 2016. The United Kingdom, Latvia and Lithuania answered that they "almost always … encounter encryption in [their] operational activities".[82] In contrast, Hungary, Slovenia and Czechia said they "rarely" encountered it,

[78] Mike Brunker "Snowden Leaks Didn't Make Al Qaeda Change Tactics, Says Report" (16 September 2014) NBC News <www.nbcnews.com>.

[79] Brunker, above n 78.

[80] WhatsApp Help Center, above n 5.

[81] Danielle Kehl, Andi Wilson and Kevin Bankston *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s* (New America, June 2015) at 18–20.

[82] Council of the European Union *State Questionnaire on the Encryption of Data* (12368/16, 20 September 2016) (results obtained under EU Regulation (EC) No 1049/2001 Request to the General Secretariat of the Council of the European Union by Mr Rejo Zenger).

while Germany asserted they did not have statistics on how often it was encountered.[83] Either way, these results fail to show a conclusive trend. These questionnaire answers may have been far more politically motivated than factually accurate. It does not seem likely that Latvians use encryption so much more than Czechs to yield these opposing results.

In Aotearoa New Zealand, there is no publicly available data on the extent of this issue. In such an environment, we must refuse to implement any privacy breaching solutions without concrete data providing demonstrable need. For now, if such data does not yet exist, it is unlikely to just materialise in the future. If not based on statistical realities, law enforcement likely have other reasons behind its objection to E2EE.

E *Just do your job: The laziness of law enforcement and intelligence agencies*

Law enforcement and intelligence agencies have become accustomed to individuals not knowing how to, or being incapable of, asserting their privacy rights in the digital space. These agencies are crying foul now that education is under way and providers are taking it upon themselves to assert rights. Instead of looking at the ways in which technology provides alternatives to catch criminals, they wish to lazily fall back into the open-access status quo. Many alternatives are available to even directly combat E2EE. Lawful hacking by exploiting vulnerabilities, such as those used by the Dutch, can be legislatively regulated as it is in the United Kingdom.[84] Lawful hacking even temporarily enabled the breach of WhatsApp's E2EE in 2019.[85]

Additionally, obtaining physical access to an end point device enables law enforcement to read plaintext messages. The German Federal Police did this with WhatsApp when they took phones and used them to grant access to that device's account on the WhatsApp web browser version on police computers, before returning phones to suspects to continue using.[86]

However, the most important of all is metadata. This is the external data compiled about a communication beyond its actual contents. Such data is collected as a by-product of a platform's functionality. It includes items such as location data, call records, platform usage records, common associates and unique phone identification. It can place a suspect at a crime scene, establish an alibi or act as a bug without the need for a physical device to be planted. In fact, metadata is so useful that a former NSA Director has admitted that the United States "kill[s] people based on metadata", and that such surveillance reveals "everything" about people, making the actual contents of communications irrelevant.[87] Even in E2EE platforms, metadata is available to the messaging provider and therefore obtainable in a usable form by law enforcement. There are considerable privacy issues surrounding this, but these are beyond the scope of this article. For now, it suffices to say that metadata provides a trove of information without needing to access the actual contents of communications.

All of these ideas go to show that law enforcement and intelligence are capable of detecting crime regardless of whether E2EE remains encrypted. As Peter Swire and Kenesa

[83] Council of the European Union, above n 82.

[84] Investigatory Powers Act, pt 5.

[85] Will Cathcart "Why WhatsApp is pushing back on NSO Group hacking" *The Washington Post* (online ed, Washington DC, 29 October 2019).

[86] Deutsche Welle "Kann das BKA WhatsApp-Nachrichten mitlesen?" (21 July 2020) <www.dw.com> (translation: "Can the BKA read WhatsApp messages?").

[87] Lee Ferran "Ex-NSA Chief: 'We Kill People Based on Metadata'" (12 May 2014) ABC News <https://abcnews.go.com>.

Ahmad put it, technology is not leading us to "go dark", but instead has ushered in "the golden age of surveillance".[88] The reasons for such protests against E2EE are possibly more psychological than practical. Behavioural economics suggest humans are more likely to "prefer avoiding losses to acquiring gains of similar value", known as the loss aversion effect, and that "people place higher value on goods they own versus comparable goods they do not own", known as the endowment effect.[89] As the hard data shows, these agencies protest too much and it is likely that they would rather accept current technology, even if it means some E2EE, rather than returning to a pre-technology era.

F *Cooperation of surveillance intermediaries*

The cooperation and actions of surveillance intermediaries are vital in any attempt to regulate E2EE. Some scholars suggest that surveillance intermediaries "know more about law enforcement requests than any other entity—including the government".[90] They are best equipped to "differentiate 'normal' requests from aberrant ones".[91] Therefore, such companies are best placed to know trends and report any concerning law enforcement request trends to an oversight body, like the Privacy Commissioner or the High Court sitting with expert lay members. Such reporting requirements would need to be added to statutes, such as the Privacy Act 2020 or the Search and Surveillance Act 2012. Information about trends and technical realities also positions technology companies in the best place to litigate complex surveillance-related privacy concerns.

There is an ever-present danger that companies may decide to remove E2EE or readily comply with requests to access private information through technological workarounds. Companies might well proceed in this fashion if they believe it is in their best interests, but ought to remember they are "private institutions with quasi-public functions".[92] To this end, such companies have responsibilities to act in good faith to protect their users' privacy interests. In many instances, good faith may well be sufficient, as shown by the amount of time, money and resources tech companies have currently invested in upholding free speech rights on their platforms.[93] Regardless, increased user privacy expectations are making privacy a central requirement to messaging and social media platforms, and therefore an essential part of their continued economic viability.

However, great danger lies in ignoring domestic legislation. The tech state is arguably unreachable and only limitedly bound by law. It may well come to the point where intermediaries could and would simply ignore technologically illogical or rights-breaching court decisions or legislation. Facebook had initially denied it was bound by Aotearoa New Zealand law, a stance directly contravening the Office of the Privacy Commissioner.[94] However, at least for now, the majority of Big Tech has yet to reach the point of no dialogue—a stance that will hopefully continue.

[88] Peter Swire and Kenesa Ahmad "Encryption and Globalization" (2012) 13 Columbia Science and Technology Law Review 416 at 466–470.

[89] At 472.

[90] "Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance", above n 28, at 1738.

[91] At 1738.

[92] At 1739.

[93] Kate Klonick "The New Governors: The People, Rules, and Processes Governing Online Speech" (2018) 131 Harv L Rev 1598 at 1618–1622.

[94] Office of the Privacy Commissioner "Facebook must comply with NZ Privacy Act" (press release, 28 March 2018).

G *Expert lay members of the High Court*

By now, the inherent technological difficulties in discussing E2EE will be apparent. Many solutions come from a failure to understand the technical realities of E2EE and what they would ultimately mean for individual privacy rights. It has been left to surveillance intermediaries, cryptographers and computer scientists to litigate and educate on the real risks of every proposal. For that reason, this article suggests the appointment of expert lay members to the High Court to provide oversight and rulings in technologically advanced cases, particularly in the E2EE space. Currently a similar power to appoint expert lay members is provided for in ss 77–78 of the Commerce Act 1986. This ensures "that expert evidence on complex competition issues is properly understood, tested and assessed by the High Court".[95] In this context, a similar provision would allow a mix of legally and technologically trained professionals to provide technologically accurate and rights-affirming oversight as enshrined in legislation. For example, this bench could authorise limited lawful hacking or the use of Trojan software where appropriate. They could also rule on whether technology companies have the technological capacity to provide decrypted information. This solution would help bridge the current difficulties faced by the ill-informed or disingenuous state and the profit-motivated private sector, while increasing judicial competence in this area.

VI Recommendations

For the reasons highlighted above, this article makes the following recommendations:

- accept that E2EE provides vital communicative privacy, and its prevalence is only expected to continue;
- conduct a review of the necessity of breaking E2EE based on available data on cases where such issues are engaged;
- adopt a strong policy preference in favour of E2EE with no support for any weakening technologies;
- enact a designated legislative regime for any E2EE workarounds, such as metadata use and lawful hacking, when compelled by a warrant;
- ensure any legislative regime has sufficient oversight from a High Court bench comprising expert lay members; and
- investigate the threats posed to individual privacy rights with respect to their sensitive metadata.

VII An Overture or Obituary for Privacy in the E2EE Era

When the first Crypto-Wars began, governments were sure this was the beginning of the end for law enforcement and national security. But nearly 30 years on, as encryption evolves, we have yet to see the sky fall in or the beginning of the end of public safety. In contrast, what we are seeing are strong challenges to weaken our communicative privacy. It is thus incumbent on us to have a robust public debate to decide whether this E2EE era calls for an overture or obituary for communicative privacy. This article substantially

[95] Ministry of Business, Innovation and Employment "Lay members of the High Court for Commerce Act cases" (25 July 2022) <www.mbie.govt.nz>.

commits to this debate and affirms the most privacy-respecting approach possible at the current state of technology. As technology evolves further, the arguments here may become less relevant, but the foundational commitments and comments about what privacy requires in the E2EE age will endure. And so, we must end as we began. We can and must address the vast extra-legal chasm currently plaguing lawmakers and judiciaries on this issue, and we must do so before emotionally clouded emergency legislation is passed in the wake of a horrific crisis.