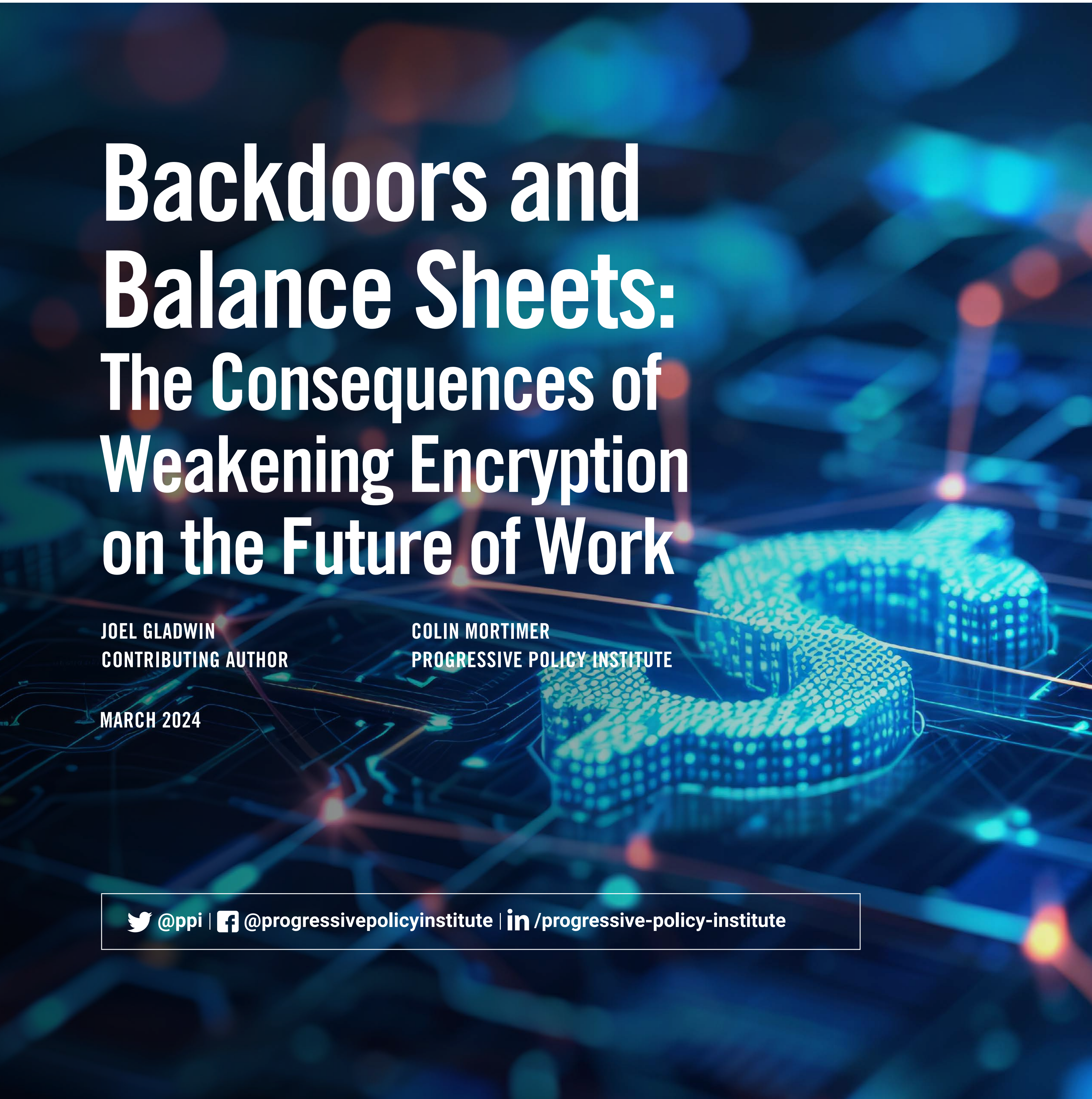
ppi radically pragmatic



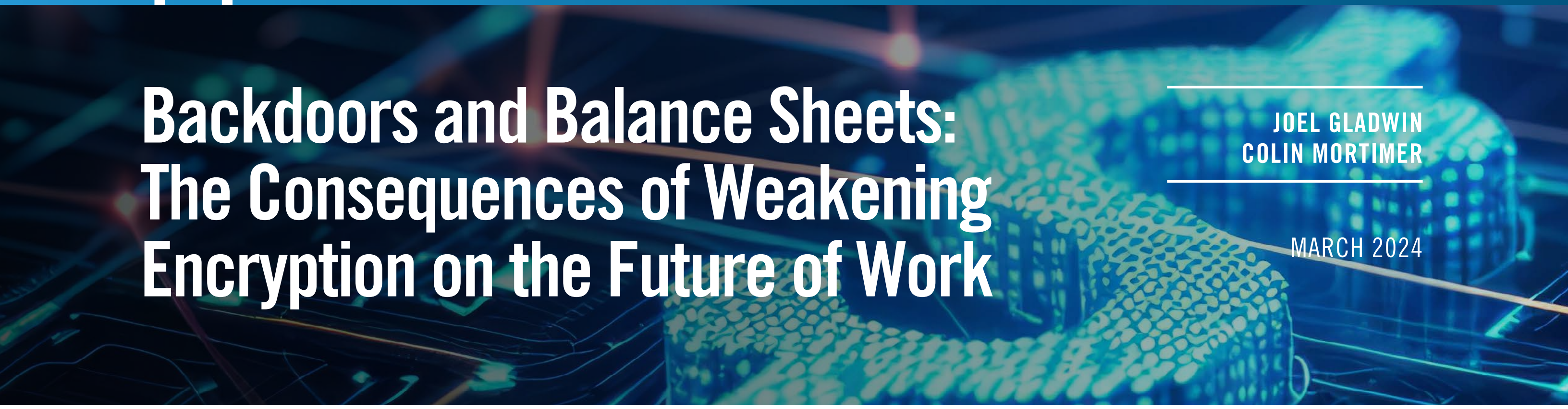
# Backdoors and Balance Sheets: The Consequences of Weakening Encryption on the Future of Work

JOEL GLADWIN
CONTRIBUTING AUTHOR

COLIN MORTIMER
PROGRESSIVE POLICY INSTITUTE

MARCH 2024

@ppi | @progressivepolicyinstitute | /progressive-policy-institute



# Backdoors and Balance Sheets: The Consequences of Weakening Encryption on the Future of Work

JOEL GLADWIN
COLIN MORTIMER

MARCH 2024

## INTRODUCTION

**While encryption protects individuals against crimes, like identity theft or unlawful surveillance, law enforcement and intelligence agencies (LEIAs) argue that encryption makes it more challenging, or impossible, for them to investigate crimes and threats to public safety.**

The Five Eyes intelligence alliance — composed of Australia, Canada, New Zealand, the United Kingdom, and the United States — has made a number of joint statements in recent years that have called for stricter regulation of encryption, including greater cooperation from technology companies that develop and use encryption in their widely used products and services.

Although different policy proposals over the years have changed the way that these debates are framed, the problem remains unchanged: there is no such thing as a backdoor that only lets the good guys in.

For too long, the encryption policy debate — both for and against — has centered around non-economic values, such as crime, privacy, and freedom of expression. While these issues certainly have economic *consequences,* that factor has been, at best, an afterthought in the debate on how this technology should or shouldn't be regulated. This is partially because measuring the economic consequences of encryption regulation is an inherently difficult task. Such regulation is generally unprecedented, or has only come into place recently, meaning that there is no result to extrapolate from.

PPI believes that the economic question of encryption ought to be a more salient part of the debate. Regulation on a piece of unquestionably innovative technology needs to be thought through by more than just a values-based analysis. For the first time, this report examines the economic impact that mandating encryption backdoors would have on small- to medium-sized enterprises (SMEs) across the Five Eyes.

Our headline findings suggest:

- 99% of SMEs utilize encryption services which are very or quite important for use internally and/or with customers.
- 62% of business leaders would reduce hiring if encryption backdoors were implemented.
- 58% of business leaders would reduce their investment if backdoors were implemented.
- 52% of business leaders believe that the global standing of their country's technology sector would be adversely impacted if backdoors were implemented.

Our analysis leads us to conclude that any attempt to weaken encryption — whether it is through front doors, backdoors, or client-side scanning — would inflict economic self-harm in the *multiple billions of dollars,* and produce negative spillovers that would amplify this globally.

The economic cost of weakening encryption, therefore, provides the illusion of protection while actually crippling the economy. We believe this is an important contribution to the debate around encryption regulation that helps to move the discussion forward,

Governments and LEIAs must cooperate better with technologists and take a more practical, incremental approach to policies and legislation that affect national security and public safety, rather than mandating encryption backdoors or ubiquitous surveillance.

## TECHNICAL OVERVIEW OF ENCRYPTION

Technology is ingrained into our daily lives. The internet is quite literally at our fingertips. Rotary phones have made way for FaceTime calls and Zoom meetings, letters have transformed into text messages and emails, and wearable devices offer real-time insights into our health, tracking heart rates, blood sugar levels, and other vitality metrics. A variety of communication technologies and the Internet of Things (IoT) have expanded our reality and keep us connected to our friends, families, and communities, regardless of where we are in the world. As we expand our use of these digital technologies, companies are hard at work making sure they remain secure, often using encryption to safeguard our data.

There are many definitions of encryption, but a simple and fairly complete one is, "any procedure used in cryptography to convert plaintext into ciphertext to prevent anyone but the intended recipient from reading that data". Of course, in the context of the issue at hand, "text" can mean any type of communication, such as voice, images, characters, video, chat, websites, and more. The intent of encryption is to provide a means to prevent others who might intercept an encrypted communication from understanding its content.

An encryption algorithm is used to take plaintext in combination with a "key" to generate a ciphertext. Decryption algorithms employed upon receipt reverse this process to reproduce plaintext, meaning that the intended recipient of an encrypted message must have the key to read that message. We should think of encryption as a system, including many elements working together across the internet. It is not just the mathematical elements instantiated in software but also a broad set of algorithms and critical functions such as secure key exchange. The assumption is that no one but the sender and the intended recipient should have the keys.

There are two main types of encryption systems. The first is symmetric encryption, which entails using the same keys to encrypt and decrypt information.[1] Symmetric encryption is typically used to protect data-at-rest.[2] For instance, it is used to protect stored files, by operating systems to protect unauthorized access to user data (full-disc encryption), and by smartphones and tablets to lock devices.[3]

The second type of encryption is asymmetric encryption where the encryption and decryption keys are different. Asymmetric encryption is typically used when data is transmitted ("data in motion"), and uses both public and private keys. So while a public key is available to everyone, a private key is only available to select individuals. In this system, a sender uses the recipient's public key to establish a secure communication channel, but only the intended recipient can receive and decrypt the ciphertext using the transmitted public key in combination with their private key.[4] This way, a sender can encrypt a message using a public key, but only the intended recipient, who is the holder of the private key, will be able to decrypt the message into plaintext.

One type of encryption that uses both symmetric and asymmetric encryption is end-to-end encryption (E2EE), which provides confidentiality for transmitted data between two endpoints on a recipient's device.[5] In E2EE, a message encrypted at its source cannot be decrypted until it reaches its intended recipient where it is decrypted. This means that no third party can access the plaintext or the decryption key.[6] Many communication protocols, including instant messaging applications like WhatsApp and Telegram, email services like ProtonMail, and Voice-over-IP (VoIP) services like Zoom. These protocols are designed so that third parties, such as service providers, do not have access to any of their users' private keys. This prevents any third party from being able to access messages in plaintext.

### How is encryption used?

Encryption is critical for keeping information secure and has existed since before the Internet age. From the cipher method used by Julius Caesar to the Enigma machine in World War II, individuals have been using encryption to protect confidential communications, trade secrets, and national security information.[7]

Companies have used modern digital encryption for the last fifty years to protect their data from breaches, as well as to safeguard their communications and operations, and many sectors (including health care, financial services, and education) have industry-specific requirements to encrypt their data, whether in laws and regulations, or through best practices and standards.

By providing these protections, encryption is a critical enabler of our increasingly digitized economy, by ensuring trust in e-commerce, financial transactions, digital health, e-learning, secure information storage, and secure private communications, and by assuring our civil liberties, such as privacy, freedom of speech, and freedom of association.[8, 9]

While some research (as we'll explore later in this paper) has tried to assign a monetary value to encryption, it is a difficult task given the manner in which it is woven throughout our modern existence, the countless ways upon which we rely on it in our daily lives, and the innumerable second and third order effects that encryption now plays in our lives. Privacy and security are now built into the products and services we use on a daily basis, and are increasingly taken for granted. It is the very foundation for trust on the internet, and it is this trust that has enabled the tremendous growth of communications, commerce, financial, and health services across the globe.

Trust via encryption is the underpinning for all of these activities on the internet, and without it, individuals and entities would not be willing to engage in these activities online. For example, the disruption of New Zealand's NZ$204 billion (USD$135 billion) stock exchange in 2020 due to a series of cyberattacks led to a loss of confidence, and trading had to be stopped because of concerns about market integrity.

As our societies continue to shift to more of an information and data economy, more encryption is needed, not less, and undermining its strength takes us in the wrong direction. Projections indicate there will be more than 29 billion IoT devices in use by 2030, including cars, smoke detectors, and home security systems, most of which will generate sensitive personal data. The next generation of breaches may not only threaten your data but also your life and those of your loved ones.

Studies completed by the US National Institute of Standards and Technology (NIST) in 2001 and 2018 concluded that government-sponsored interventions that improved consumer trust in digital security resulted in aggregate benefits worth many billions of dollars.[10] And the Centre for Economics and Business Research (CEBR) has found that a 5% point increase in digital trust results in an average increase in GDP per capita of $3,000 across the world.[11]

Despite remarkable advances across the digital landscape, the same features of encryption that make it a critical part of the internet can be utilized by criminals and malicious actors to hide illegal activities across a number of applications. Law enforcement and national intelligence agencies (collectively termed LEIAs) across the Five Eyes have worried for decades that encryption is preventing them from doing their jobs, pointing the blame at technology companies.

The LEIA's calls have been pretty simple: establish a system that gives them exceptional access to encrypted material and scan messages to identify harmful content. They claim that this would help protect children, keep illegal drugs off the street, prevent corruption, and potentially stop violent crimes and terrorism. But as we shall see, these overly simplistic solutions have the potential to inflict tremendous economic self-harm by degrading the system of trust and privacy that enables our modern digital economies to flourish.

### How did we get here?

The policy debate surrounding encryption and tensions between national security and privacy are long established.[12, 13] However, the nature of this debate has evolved over time: beginning with a focus on key escrow mechanisms, followed by a push towards counter-terrorism capabilities by Five Eyes' intelligence agencies, and, more recently, proposing means to weaken encryption in order to combat child sexual abuse material (CSAM).

Arguments against modern digital encryption pre-date the internet, and played a significant role in the Cold War. Following World War II, the United States placed export controls on encryption technologies for communication, which banned the export of strong encryption technologies. Other Five Eyes governments also followed suit, considering them to be munitions or having dual-use military applications.[14]

But as public demand for strong encrypted communications grew alongside the adoption of the internet, law enforcement and intelligence agencies (LEIAs) recognized this new demand for user security but were cautious of jeopardizing their surveillance capabilities to access communications.

### *First Crypto War (1990-2000)*

The "First Crypto War" was characterized by a focus on building backdoors into encrypted systems which would enable user security without detracting from investigatory objectives. This included the USA's "Clipper Chip" proposal in 1993, which would have allowed the intelligence agencies to obtain access to encrypted communications on any device.[15] The chip would use key escrow, a concept that enables a third party — in this case, the government – to access a decryption key to read encrypted content. This escrow proposal was defeated in 1999 due to pressure from civil society organizations and academic consensus that key escrow was easy to exploit and, therefore, not secure.[16]

In response to this, the Organisation for Economic Cooperation and Development (OECD) issued a set of guidelines for cryptography policy, which acknowledged the need for strong encryption, and required any lawful access measures to respect privacy rights and the confidentiality of information systems.[17]

### *Second Crypto War (2010-2018)*

Following the Snowden disclosures in 2013, which revealed the interception capabilities of state actors such as the US National Security Agency (NSA), encryption tools became more pervasive amongst companies and individuals seeking to protect their privacy and data security. Resultantly, the debate surrounding cybersecurity, and privacy, and national security rematerialized as the "Second Crypto War".

This time, the LEIAs, such as the US Federal Bureau of Investigations (FBI), presented the "going dark" narrative; namely the widespread use of encryption had inhibited their ability to lawfully gain access to tackle terrorism and other serious crimes. Thus, the debate did not focus on specific backdoor mechanisms like the First Crypto War, but marked a clear stance that greater access to encrypted data was necessary.

This narrative prompted a regulatory push for solutions to this going dark issue, particularly by the Five Eyes intelligence agencies. Canada's 2016 National Security Consultation flagged encryption as an intelligence challenge that motivated the government's agenda for reform.[18] There was also a concerted drive across the Five Eyes to compel technology companies to provide technical assistance in their investigations by decrypting communications.

For instance, the UK and Australian governments went the furthest by passing legislation to compel companies to comply with technical assistance and capability notices. And in 2016, the FBI issued a court order on Apple to break the security of an iPhone during the investigation of the San Bernardino shooting, in an attempt to track down additional leads. Apple strongly opposed the order on the grounds that it would essentially create a backdoor and undermine encryption on the iPhone. In the end, the FBI gained access to the device through a third-party, but they did not find any new information for their investigation.

### *Recent Developments (2020-Present)*

Recent developments have brought to the fore newer "workarounds" to weakening encryption, further complicating the tensions between privacy and public safety. Client-side scanning has increasingly emerged as an alternative to other backdoors, and as a justified means to combat CSAM.

Also known as endpoint filtering or local processing, client-side scanning scans the encrypted content  (e.g. images, videos, files, etc.) before they are sent or received to check against a repository of illegal content.[20] The application responsible for the client-side scanning then reports to a third party whether the scanned content matched anything in the repository.[21]

In 2021, Apple announced that it was developing a new CSAM scanning technology.[22] This on-device matching technology would use cryptography to detect known CSAM images before they were stored in iCloud Photos by cross-examining them with a database of known CSAM hashes.[23] Although the company attempted to proactively develop a technological solution that would protect user privacy whilst finding illegal content, the risk of client-side scanning is that it could be used without authorization and amounts to a security backdoor.[24]

After years of research, Apple determined that "[s]canning every user's privately stored iCloud data would create new threat vectors for data thieves to find and exploit. It would also create the potential for a slippery slope of unintended consequences. Scanning for one type of content, for instance, opens the door for bulk surveillance and could create a desire to search other encrypted messaging systems across content types."

As we have seen, throughout the encryption debates, several proposals have surfaced from backdoors and front doors into encryption algorithms and content, as well as discussions around making strong encryption illegal.

| PROPOSAL | WEAKNESSES |
|---|---|
| **KEY ESCROW:**<br>A method whereby encryption keys are held by a trusted third party, allowing law enforcement access to encrypted data when certain conditions are met. | • The security and trustworthiness of third parties could result in unnecessary risks (e.g., misuse, unauthorized access).<br>• Targets on keyholders could result in catastrophic attacks.<br>• Rapid access to data is difficult when keys must be reassembled or transferred. |
| **UNMEDIATED ACCESS:**<br>The deployment of tools and techniques by law enforcement to gain access to encrypted data without involvement from the data owners or processors. | • Backdoors used by law enforcement may also be exploited by malicious actors or abused for unauthorized uses.<br>• Access to data without the knowledge or consent of data subjects could represent a variety of privacy, civil rights, or civil liberties issues. |
| **TECHNICAL ASSISTANCE:**<br>The process through which a tech company may be compelled to help law enforcement access encrypted data by weakening encryption or creating tools to decrypt data. | • Creating tools or backdoors weakens systems, making them more vulnerable to attacks.<br>• Companies may lose their users' trust if they believe their products are intentionally weakened for law enforcement.<br>• Companies may build weaker systems by default in anticipation of compliance requirements. |

Although proposals over the last few years have changed the way that these debates are framed, the problem remains unchanged: **there is no such thing as a backdoor that only lets the good guys in.**

The security afforded by encryption is only as strong as its implementation. Strong encryption should be thought of like a strong bank vault, both of which make gaining access to what is inside impractical, in that it would take too much time, money, resources, and/or expertise to break the encryption just as it would to break into the vault. If an encryption algorithm is weakened, then the plaintext could be recovered fairly readily by an interceptor. A weak algorithm is like an unsophisticated lock on the vault, but a strong lock on the vault is useless if you can just cut through the hinges and lift the door off.

All the parts of the encryption system must contribute to its strength. With increasingly strong encryption, it becomes very difficult, approaching impossible, to break the encryption. It is also crucial to ensure that private keys are only distributed to their intended recipients, not any other third parties who could use, misuse, or lose them — this includes the government. If criminals know that there is a key store, or that an encryption algorithm has a door they can unlock, then that will prove to be a honeypot to criminals, who will do their best to unlock it for their own ends.

In 2017, the CIA experienced the "biggest unauthorized disclosure of classified information" in the agency's history due to "woefully lax" security measures (this incident is known as "Vault7"). As a result, the CIA shuttered intelligence operations that exploited vulnerabilities in systems.[25] Similarly, the Shadow Brokers, a criminal enterprise, compromised the NSA and released stolen vulnerabilities that existed in Microsoft's software. Malicious actors would later weaponize those vulnerabilities by creating the WannaCry and NotPetya ransomware,[26] which caused billions of dollars of damage worldwide.[27] So to take the analogy further, even the strongest of vaults will open if you gain access to the keys.

## ENCRYPTION POLICY AND LEGISLATION ACROSS THE FIVE EYES

The Five Eyes intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom, and the United States have made a number of joint international statements that call for stricter regulation of encryption, including greater cooperation from technology companies that develop and use encryption in their widely used products and services.

Recently, the Five Eyes alliance, together with India and Japan, released an international statement on end-to-end encryption where they called on technology companies to design or modify their encrypted messaging services to permit law enforcement to intercept and gain access to decrypted or plaintext copies of users' communications.

### The United Kingdom

The UK has been the most active Five Eyes government to try and proactively legislate for greater powers to compel companies to decrypt communications, or weaken the encryption of their services. This forceful approach can at least in part be traced back to the UK's long history of state surveillance, in particular the capabilities developed during the Second World War to decrypt signals.

The most significant law is the Investigatory Powers Act 2016 which allows the government to issue a "Technical Capability Notice" (TCN) to any communications operator (which includes telecommunications companies, internet service providers, email providers, social media platforms, cloud providers and other "over-the-top" services), whether UK-based or anywhere else in the world.

This can include the provider having to remove "electronic protection applied by or on behalf of that operator to any communications or data." The Secretary of State must also consider technical practicalities, such as whether it is "practicable" to impose requirements on operators, and for the operators to comply. Section 254 provides that Judicial Commissioners conduct a necessity and proportionality test before approving a TCN. This means that a provider receiving a TCN must be able to centrally manage encryption and maintain the decryption key.[28]

Separately, the UK government passed the Online Safety Act in September 2023.[29] The Act is designed to keep social media platforms and other internet-based services free of illegal and harmful material. The law applies to a broad set of online service providers, including search engines, social media platforms, hosts for user-generated content, online forums, games, and pornography sites.

Although the Act does not ban E2EE explicitly, it does require content filtering and age verification using government-approved technologies. The proposal also included a provision that would force tech companies providing E2EE messaging to implement client-side scanning technology to monitor CSAM so it can be reported to authorities.[30] This was met with strong opposition from civil society and privacy groups, and an additional amendment was included which stated that companies will not be required to scan encrypted messages until it is "technically feasible and where technology has been accredited as meeting minimum standards of accuracy in detecting only child sexual abuse and exploitation content".[31] But as we have already explored, there are divergent opinions between law enforcement and technologists about whether this will ever be technically feasible without weakening encryption.

Signal, the popular messaging app, has stated that it will stop operating in the UK market if encryption backdoors are required.[32] The UK Home Office also operationalized a public campaign against Meta rolling out E2EE for Facebook and Instagram, using graphic language to describe CSAM that they believe might go undetected. A video featured a victim of child sex abuse appealing directly to Meta's CEO, Mark Zuckerberg, to rethink plans to roll out encryption.[33] After the Online Safety Act passed, and despite pressure from the UK Home Office not to,[34] Meta launched its long-planned E2EE for Messenger,[35] joining their encrypted WhatsApp product, and it will continue to monitor its platforms for grooming and the sharing of child abuse content using methods that don't require that they peer into every message on their platform.[36]

In response, the Home Office decided to update the IPA through an Amendment Bill in November 2023, which will place broad requirements around extraordinary access, and includes new powers for the government to pre-approve or block new security technologies that could impact the global market.[37] Clause 20 introduces a Notifications Notice, requiring operators who are issued with such a notice to notify the Home Office of plans to make product or system changes in a way that could impede investigations, including the introduction of security features like E2EE. If used in combination with the new power to order the maintenance of the status quo during any TCN referral process, these changes would, in effect, grant a de facto power to indefinitely veto companies from making changes to their products and services offered in the UK.

Similarly, the extraterritorial nature of the IPA could essentially allow the UK government to require foreign companies to take actions that might conflict with their own national laws, placing private companies in an untenable position of having to decide which country's law to comply with. This new regime would place additional obstacles on innovation and security updates, which would undermine the quality of British technology services, and place the UK at a competitive disadvantage. The Amendment Bill is expected to become law by Spring 2024.

It is unclear whether the provisions within the IPA would withstand such a challenge before the European Court of Justice on the basis of incompatibility with the European Convention on Human Rights (ECHR), especially Article 6 (right to a fair trial) and Article 8 (right to privacy).

### Australia

The UK is not alone in its attempt to curb the use of encryption through legislation. Australia passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA) in a bid to equip law enforcement and intelligence agencies with the tools required to effectively operate in the digital era and address terrorism and crime.

The Act increased responsibilities for communication service providers, businesses, or individuals involved in manufacturing equipment, developing or updating software, or operating websites to cooperate with law enforcement and security agencies. It also created computer access warrants for law enforcement and bolstered security agencies' search and seizure authority for accessing account-based data via a search warrant and for unencrypted data on computers and mobile devices.

Taking inspiration from the UK's IPA, three new mechanisms were introduced into the Telecommunications Act: Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs). TARs can be issued by Australian security agencies that may "ask the provider to do acts or things on a voluntary basis that are directed towards ensuring that the provider is capable of giving certain types of help". TARs escalate to TANs compelling assistance and impose penalties for non-compliance. The Australian Attorney-General can also issue TCNs which "may require the provider to do acts or things directed towards ensuring that the provider is capable of giving certain types of help" or to actually do such acts and things.

While the language of TCN is similar to the UK IPA, there is a much longer list of "acts or things" that a provider can be asked to do upon receipt of a TCN. Although it makes clear that a "systemic weakness" cannot be introduced, there is still a significant potential impact on the security and privacy of encryption. Another important distinction is that the Australian TCN's are issued by the executive, with limited access to judicial review.

The Act received a lot of criticism from civil society, human rights groups, and the general public regarding the speed of its passage, a lack of transparency, and a poor consultation process. Although safeguards built into the law maintain that nothing can require industry to break encryption, critics maintain that the law's ability to create new capabilities may be used to compel companies to weaken encryption or build backdoors.

Given the extra-territoriality of the TOLA, both from a company geography perspective as well as powers to help Australian law enforcement assist their foreign counterparts; there are legitimate fears that these provisions could operate as a loophole through which foreign law enforcement agencies circumvent their own legal system's safeguards and capitalize on Australia's lack of a federal human rights framework. As of June 2020, no compulsory orders have been issued and fewer than 20 assistance requests were drafted.[39]

In another striking similarity to the UK Online Safety Act, the draft standards issued by the Australian eSafety Commissioner included a range of proactive detection obligations on digital services to scan content in order to detect, remove, disrupt, and deter CSAM and "pro-terror" content. Hashing, artificial intelligence, and client-side scanning were specifically referenced without any safeguards for E2EE.[40] Considering that this is technically impossible to implement without weakening encryption, in a similar vein to the UK's attempt, the eSafety Commissioner has clarified that operators of cloud or messaging services must detect and remove known child abuse material and pro-terror material "where technically feasible", and it "does not advocate building in weaknesses or back doors to undermine privacy and security on end-to-end encrypted services".[41]

Where something is deemed to not be technically feasible, the eSafety Commissioner has said the standard would require other measures, including clear and identifiable user reporting mechanisms, and detecting patterns in the behavior of users – not including reviewing encrypted communications. However, these remarks offer little legal protection as they were not made explicit in the draft standards.

### United States

The legal situation in the US to compel decryption depends, at least in part, on the actor targeted. The US has no specific legislation (as of yet) dealing with encryption although other laws on government investigatory and surveillance powers may be applicable. Forcing an individual to decrypt data or communication has generally been considered incompatible with the Fifth Amendment in the US Constitution (i.e. right to self-incrimination), although there is no authoritative Supreme Court decision on the issue.[42]

For communications providers, the US has a provision in the Communications Assistance for Law Enforcement Act (CALEA) on Capability Requirements for telecommunications providers, which states that providers will not be required to decrypt or ensure that the government can decrypt communications encrypted by customers, unless the provider has provided the encryption used.[43] Litigation has been initiated against companies that refuse to provide assistance; the most notable being the FBI-Apple dispute concerning the locked iPhone of one of the San Bernardino shooters. Ultimately, the FBI was able to unlock the iPhone without Apple's assistance, by relying on a technical solution from Cellebrite, thereby engaging in a form of "lawful hacking."

Over recent years, there have been a number of legislative efforts to weaken encryption through the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT) Act. This Bill has already failed twice before in 2020 and 2022, due to overwhelming public outcry and opposition from human rights groups, but it was reintroduced for a third time in May 2023. The authors of the EARN IT have stated that the goal of the Act is to encourage companies to increase their client-side scanning of users' files and communications. EARN IT would force companies to continuously monitor their users' data by removing Section 230 protections from companies which currently affirms that users, not services, are liable for what they post online and shield services from liability over their content moderation decisions.[44]

In essence, the Act could force companies into protracted legal battles over whether continuing to use encryption is "knowingly reckless behavior" by failing to prevent CSAM on their services. If a platform should have known that there was CSAM, then the government could argue that its use of E2EE was reckless and contributed to its failure to prevent the presentation and distribution of CSAM on its service, and thus is punishable under the EARN IT Act. Because online services that use E2EE cannot scan encrypted content without undermining the confidentiality of users' data, EARN IT would essentially compel companies to remove encrypted services entirely, weaken encryption in their offerings, or face endless litigation and harsh legal risks.

### Canada

Canada does not have specific legislation (as of yet) that provides authorities the power to compel decryption. Canadian authorities have imposed requirements on wireless communications providers through spectrum licensing conditions in the form of the Solicitor

General's Enforcement Standards for Lawful Interception of Telecommunications (SGES) Standard 12, which obliges providers to decrypt any communications they have encrypted on receiving a lawful request, but excludes E2EE "that can be employed without the service provider's knowledge."

It appears the requirements only apply to encryption, do not require the operator to develop "new capabilities to decrypt communications they do not otherwise have the ability to decrypt", and do not prevent operators from employing end-to-end encryption.[45]

There are provisions of the Canadian Criminal Code which give operators immunity from civil and criminal liability if they cooperate with law enforcement "voluntarily" by preserving or disclosing data to law enforcement, even without a warrant. There are also production orders and assistance orders that can be issued under the Criminal Code to oblige third parties to assist law enforcement, and disclose documents and records which could, in theory, be used to target encrypted communications, but legal experts cast doubt on this.[46] There are also practical limitations, including the fact that many digital platforms and services do not have a physical presence in Canada, and thus are effectively beyond the jurisdiction of Canadian authorities.

The Canadian Charter of Rights and Freedoms has a number of sections relevant to how undermining encryption can interfere with democratic freedoms, namely sections 2 (freedom of expression), 7 (security of the person), 8 (right against unreasonable search and seizure), and the right to silence and protection from self-incrimination contained in sections 7, 11 and 14. Case law from Canadian courts suggests that individuals cannot be compelled to decrypt their own data.[47] The Charter implications of BlackBerry's assistance to the Canadian police in the R v Mirarchi case was never ruled on as the case was dropped.

Following in the footsteps of their Five Eyes counterparts, the Canadian government unveiled its Online Harms Act (Bill C-63) in February 2024. The proposed bill identifies seven types of harmful content, focusing on protecting children and society from sexual exploitation, violence, terrorism, and hate crimes. It places new responsibilities on social media firms to reduce exposure to harmful content, implement safety measures, and enhance transparency. Unlike the UK and Australian regimes, private and encrypted messaging platforms are explicitly excluded from the Canadian Online Harms Act.

In the absence of a legislative proposal before the Canadian Parliament, it is difficult to assess how anti-encryption powers would run up against human rights protections. But any proposal would almost certainly face scrutiny in the courts given the impacts on Canadians' Charter-protected rights.

### New Zealand

In New Zealand, provisions in the Telecommunications (Interception Capability and Security) Act 2013 (TISCA) require network operators to ensure that their networks can be technically subjected to lawful interception.[48] Although there are provisions to require public telecommunications networks to decrypt communications carried by its network, Subsection 10(4) states that an operator is not required to decrypt communications that have been encrypted using a product supplied by another entity, and the operator is not under any obligation to ensure that a surveillance agency has the ability to decrypt communications.

There is a further provision in Section 24 of TISCA that places both network operators and service providers (defined as anyone, whether in New Zealand or not, who provides a communications service to an end user in New Zealand) under obligations to provide "reasonable" assistance to surveillance agencies with interception warrants or lawful interception authorities, including the decryption of communications, when they were the source of the encryption. Otherwise, companies do not have to decrypt encryption they have not provided nor "ensure that a surveillance agency has the ability to decrypt any telecommunication". It is unclear what "reasonable assistance" entails, and how that would apply to third-party providers (e.g. WhatsApp), and it is also unclear how this provision would be enforced against offshore companies.[49]

New Zealand has human rights protections enshrined in its Bill of Rights Act 1990, and the right to privacy was established in the Privacy Act 2020. The nation's legal system also has a "relatively strong approach to unincorporated treaties, including human rights obligations."[50] Despite being part of the Five Eyes communique on encryption mentioned above, New Zealand appears to have adopted a deliberative and cautious approach to the subject, especially in comparison to the forceful push for legislation in the UK and Australia.

Nevertheless, following the Safer Online Services and Media Platforms consultation in 2023, the Department for Internal Affairs is expected to publish draft legislation in 2024. Whilst there are no explicit plans to use legislation to weaken encryption as of yet, the New Zealand government has made it clear that they expect to align the Bill closely to the UK and Australian Online Safety Acts (both of which contain powers for weakening encryption through the potential mandating of client-side scanning in the future).[51]

## A COST-BENEFIT ANALYSIS FOR POLICYMAKERS

To produce an accurate picture of how encryption affects security and public safety, we must assess the net effect. Being able to obscure confidential data and communications can be seen to have both positive and negative effects. The benefits accrue in cybersecurity, privacy, and economic growth, while the costs are said to accrue in decreased state surveillance and law enforcement capabilities. What policymakers must understand is that there is no universal solution, no silver bullet, and no magic wand capable of weakening encryption without socio-political and economic costs.

### Criminal investigations

While encryption is recognized as being a necessary safeguard to forestall data breaches, governments and LEIAs view it as an impediment to criminal investigation procedures. Among these procedures include: gathering evidence,[52, 53] prosecuting criminal offenses,[54] and preventing or detecting criminal activity.[55] The criminal activity reported spans organized crime, drug and human trafficking, and increasingly at the turn of the century, the production and dissemination of CSAM.

The prevailing justification to investigate child-related crimes stems from the profusion of new technologies that can aid the distribution of CSAM. Overall, the recurring theme across the board is the claim by national governments and LEIAs that their ability to track and investigate criminal activity is "going dark" due to the rising use of encryption technologies.[56]

Following this reasoning, weakening encryption would remove this barrier and enable LEIAs to access encrypted data to help solve criminal investigations. While this seems entirely plausible, there are a multitude of other ways that law enforcement can prosecute criminals without weakening encryption. In a survey of law enforcement officials, the Center for Strategic and International Studies (CSIS) found that the inability to identify service providers with relevant data — much of which is not encrypted — was the biggest problem in terms of their ability to use digital evidence in their cases.[57]

This knowledge and skills gap has real-world implications, which potentially contributes to the unrealistic expectations regarding backdoors as a silver bullet when it could end up dominating time and resources through false positives. For example, the European Commission admitted internally that extending scanning from known bad images to suspect images might produce a false alarm rate of 10%,[58] which would mean Europe's 1.6 million police officers would each have to take the time to investigate 625 false positives every day. Such a system would be simply unworkable.

And while some statistics have been published about the number of encrypted devices in custody of U.S. officials, this data is not entirely useful.[59] Was the encrypted data critical? Could it have been accessed in other ways? What is the likelihood that any encrypted information would have actually contributed to the case?

In the San Bernardino case in 2016, the FBI's Investigator General found that the agency had not thoroughly tried to access the phone before asking the courts to compel Apple to hack it.[60] Often there may not even be information on those devices that would have helped law enforcement to begin with. After all of the controversy around the San Bernardino case the FBI did not glean any helpful information from the device.[61] The reality is that the digital world has provided investigators with a vastly more sophisticated toolkit for solving crimes than ever before.

In many cases, specific message contents may not be needed. Greater use of metadata and traffic analysis can provide additional investigative avenues to law enforcement. Metadata can include geolocation data, device identifier information, and time, all of which are unencrypted and can be linked to an individual's identity. As we've explored, all of the Five Eyes LEIAs have the legal power to obtain various types of metadata from encrypted services, and there are numerous recorded instances of them using easily accessible metadata to investigate crime.[62,63,64]

Similarly other technological means already exist that enable LEIAs to "lawfully hack'' encrypted data. As previously mentioned in regard to the *Apple v. FBI* case, encrypted data-at-rest can be subject to "brute force attacks" which the FBI carried out after purchasing a third-party tool. Encrypted data-in-transit protocols like SSL/TLS operating on web servers can also be weakened via "man-in-the-middle attacks," whereby vulnerabilities in software and hardware are exploited by state actors which enables the plaintext to be read. A successful case of this was Operation Pacifier in 2015, where vulnerabilities in the Tor browser were exploited to identify users of the CSAM portal, Playpen. This investigation identified 8,000 computers that had been used to access the portal in 120 countries.[65]

Although “lawful hacking” raises issues relating to privacy, due process, and the fundamental rights of individuals, it does show there are viable alternatives to the restriction of encryption or weakening it through exceptional access proposals.

### National & Cyber Security

LEIAs quite regularly advocate for weakening encryption on the grounds of “moral necessity” and argue that in “ticking time bomb” scenarios like terrorist attacks, the trade-off of weakening encryption is not between privacy and law enforcement but between data protection and human life. For instance, the 9/11 attacks were in part attributed to the terrorists being able to leverage the protections afforded by encryption to coordinate plans undetected.[66] These incidents present a case for governments and LEIAs to request lawful access to encrypted content and devices within specific bounds.

Whereas certain positions advocate a balance between national security and individual rights, a pro-weakening encryption stance argues that physical security and the preservation of human life must not be subjugated by individual rights or privacy. The rationalization being that such rights can only be enjoyed in a “peaceful and secure” environment. The Five Eyes has progressed the exceptional access debate on this basis. According to a 2019 communique issued by the Five Eyes, services designed to prevent access to “terrorist and extremist material” endanger citizens and society.

But in pursuit of non-state actors, weakening encryption would open up new national security threat vectors, both directly and indirectly. It directly creates new vulnerabilities in a nation’s data security infrastructure, which increases the attack surface for adversarial state and non-state actors to exploit, leaving systems vulnerable to attacks that threaten national security.

It also leaves intelligence agencies conflicted on how they pursue their multiple missions. One mission is to collect and analyze intelligence, including the communications of foreign nationals. In this mode, intelligence agencies favor weak or no encryption, because that enables their collection and analysis mission. Another mission, however, is “information assurance”: actors such as the NSA and the UK Government Communications Headquarters (GCHQ) are responsible for securing both governmental and private sector data and communications. As the head of GCHQ put it, “Information assurance is at the heart of everything we do. And I am accountable to our Prime Minister just as much, if not more, for the state of cyber security in the UK as I am for intelligence collection.”

Complicating matters further, governments from the US to China are already making strides toward quantum computing, which can potentially break any encryption used today. And, while these breakthroughs often stay in the exclusive use of governments for short periods, inevitably they trickle down to non-state actors. To protect everyone, companies must be incentivized to constantly pursue better and stronger forms of protecting data if they have any hope of being prepared to face evolving generations of would-be criminals.

It is also evident that one nation’s encryption policy can directly impact another nation’s public policy, which in turn can impact national security. The political fallout from Edward Snowden’s revelations of the US government’s surveillance efforts was extremely far-reaching. Wider allies, like the Netherlands and Germany, called for "more and better encryption" due to their fear of the Five Eyes' ability to collect the electronic communications of their citizens. While other states ceased using the US-backed Dual_EC_DRBG encryption standard. As a Chertoff Group report put it, "by driving actors away from American products and systems we might have the perverse effect of driving internet traffic and technology companies offshore, depriving our analysts of valuable metadata information [for intelligence gathering]".[67]

Differing encryption laws across countries could also complicate treaties that facilitate transnational law enforcement cooperation, such as mutual assistance treaties. Inconsistent legislation and agreement could have implications by creating loopholes for violations as well as "jurisdiction forum shopping," a term for collaborating with overseas LEIAs as a way of circumventing national rules. When Australia passed the AA in 2018, there was widespread concern across the international community that Five Eyes' members would use Australia as the go-to place to undermine encryption. As a result, the law was reviewed months after the legislation was passed.

Regulatory arbitrage works both ways. If a lesser Western ally were to weaken their domestic encryption standards, this could be exploited by foreign adversaries. If anything, Five Eyes governments should be leading the pack by advocating for strong encryption in order to ensure wider resilience across the West at a time of increased geopolitical instability.

### Human Rights & Privacy

The right to privacy, protected by Article 12 of the Universal Declaration of Human Rights (UDHR), is supported by the availability and use of strong encryption. It guarantees that an individual's private communication and information will be secure. In addition, encryption is closely associated with freedom of expression, enshrined in Article 19 of the UDHR, along with privilege against self-incrimination under Article 6 of the European Convention on Human Rights (ECHR).

In an age where communication progressively occurs online, strong E2EE affords the integrity and security of digital interactions. Encryption is critical for the work of human rights advocates, journalists, and others who criticize state actors and therefore face heightened surveillance risks. Additionally persistent internet censorship threatens the rights to freedom of expression and assembly.[68]

Hand in hand is the concern that encryption backdoors could be exploited by those in positions of authority to oppress political opponents, religious groups, ethnic minorities, and the LGBTQ+ community. Encryption plays a crucial role in protecting the free speech of vulnerable populations, including dissidents in authoritarian countries or persecuted populations. Many technology companies have historically chosen not to comply with demands with human rights implications. For example, turning over data about users' sexuality or political activity or affiliations can carry significant penalties.

There are several options for tech companies when it comes to backdoor mandates. They could treat all governments the same way, which would make them complicit in human rights abuse. Or they could evaluate each request on a case-by-case basis without full information and the possibility of enabling human rights abuses.[69]

Encryption embodies the virtues of a liberal democracy in technological form. If Five Eyes members implement laws that threaten strong encryption, less-democratic states will feel emboldened to follow suit, and the West will lose all moral authority to criticize these regimes when it is inevitably wielded as a tool of oppression and subjugation. We've already seen this take place. Having previously backed off their demands for backdoors in encryption, the Chinese government watched the outcome of the Apple-FBI debate closely before legislating against encryption in 2017. Vladimir Putin also approved laws to a similar effect the year prior.

### Economic Impacts

Encryption secures financial transactions, preserves sensitive information, and preserves public trust in the digital marketplace. It instills confidence and trust in consumers that the service they are using is secure from data breaches and that their data will not be improperly accessed by the state. This would be undermined if encryption was weakened, either by backdoors being built into the system, or companies being compelled to provide the state with technical assistance.

Installing backdoors would also create vulnerabilities that could be exploited to commit crime-crime. Cyber attacks include security breaches, theft, or loss of customer or corporate data which can have significant economic impacts. According to an IBM study that covered 17 different countries and regions, the average total cost of a data breach to a business was $5.08 million in 2022.[70] It would also disincentivize innovators from creating new products and services because of the financial risks associated with data breaches (i.e. through fines or compensation).

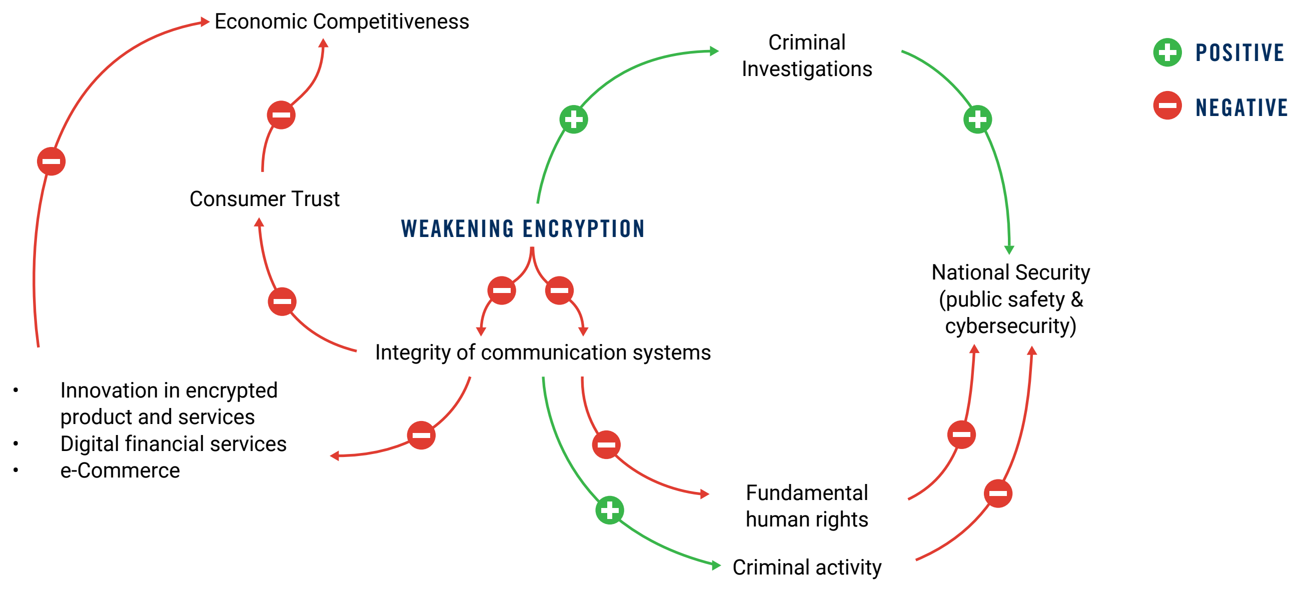
Weakening encryption is likely to affect the competitiveness of individual companies, industries and countries. Consumers generally desire the privacy protections afforded by E2EE, and it is also a selling point for American products in European and Chinese markets.[71] Mandates that weaken encryption would negatively affect the attractiveness of a company's products and services.

If regulations to weaken encryption were present in one country, a potential loss of customers or compliance difficulties might influence a company to move to another country where such regulations do not apply. Any multinational company would prefer international regulatory alignment over incoherent technical requirements across markets. Arbitrage on encryption standards could also influence a consumer's decision to stop using a product or lead a company to withdraw its operations from a country.

Finally, a country's decision to implement encryption regulations could have repercussions on international trade and trade agreements. For example, there is a prohibition in the Trans-Pacific Partnership (TPP) that prevents parties from requiring access to a commercial product's encryption-based technologies as a condition of manufacture, sale, or use unless a sale to the party's government.[72] Similarly, any business that targets European consumers must comply with EU regulations.[73] General monitoring of EU citizens is strictly prohibited under Article 8 (right to privacy) of the ECHR, and data breaches carry huge financial penalties under GDPR.

As Figure 1 shows, the issue linkages explored in this cost-benefit analysis display that the economic costs of weakening encryption provide the illusion of protection while actually crippling the economy.

FIGURE 1:


Economic Competitiveness
Criminal Investigations
⊕ POSITIVE
⊖ NEGATIVE
Consumer Trust
WEAKENING ENCRYPTION
National Security (public safety & cybersecurity)
Integrity of communication systems
• Innovation in encrypted product and services
• Digital financial services
• e-Commerce
Fundamental human rights
Criminal activity

## THE ECONOMIC COST OF ENCRYPTION BACKDOORS

For years, much of the encryption policy debate – both for and against – has centered around non-economic values, such as crime, privacy, and freedom of expression. While these issues certainly have economic consequences, that factor has been, at best, an afterthought in the debate on how this technology should or shouldn't be regulated. This is partially because measuring the economic consequences of encryption regulation is an inherently difficult task. Such regulation is generally unprecedented, or has only come into place recently, meaning that there is no result to extrapolate from.

There have been no prior empirical studies that estimate the costs or benefits of encryption regulation, and even the impact assessments produced by the UK and Australian governments do not contain any cost estimates beyond those that are administrative. Third-party empirical research is also scarce because regulation of this sort is generally unprecedented, or it has only come into place recently, meaning that there is no data to extrapolate from.

PPI believes that the economic value of encryption ought to be a more salient part of the debate. Regulation of arguably the most important technology for the global digital economy needs to be more thought through than just a values-based analysis.

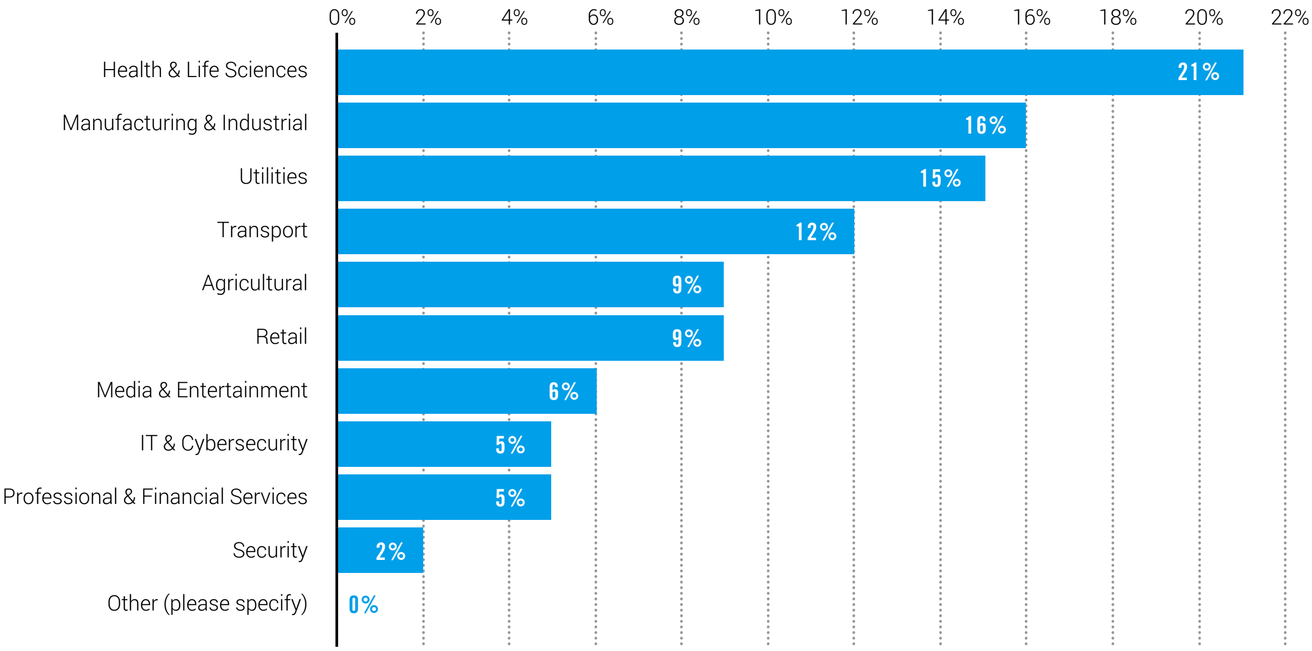
To get at this question, PPI undertook a survey of business leaders across all of the Five Eyes countries. While much has been said on how encryption regulation will affect large tech companies, less has been said on how these regulations will impact small- to medium-sized enterprises (SMEs). Thus, our survey focused on this segment of the economy to understand how these regulations may or may not impact them.

The survey was composed of a population-weighted sample of 100 business leaders in all of the Five Eyes countries — United States, Canada, United Kingdom, Australia, and New Zealand —

with a minimum of 10 respondents per country. Each business leader has knowledge of his or her company's encryption practices and capabilities. The median business leader was part of an organization with 100 to 249 employees.

Below is a figure illustrating the broad range of industries represented in the survey:

### FIGURE 2: WHAT INDUSTRY DO YOU PRIMARLY OPERATE IN?



*Source: Beresford Research*

Survey respondents overwhelmingly indicated that encryption services and capabilities were very or quite important for their businesses in multiple ways — for both communications (data in motion) and stored data (data at rest) for use internally and in business dealings with upstream vendors/suppliers and customers. 99% of respondents indicated that encryption services were very or quite important for at least one usage category.

These results are indicative of the widespread dependence on encryption services by all kinds of businesses across the economy and of the potentially tangled web of repercussions that may be transmitted across firms across the Five Eyes and internationally if the encryption capabilities of even a subset of firms are threatened. For instance, the cost of a four-week digital interruption due to a widespread cyber-attack would cost 1.5% of Australia's annual GDP, and 3.1% of the UK's GDP.

Backdoors of any kind would create technical vulnerabilities that could be exploited to commit cybercrime. This would render products and services across the entire digital economy to cyber-attacks, including data breaches, and theft or loss of customer and company data. The majority of respondents to our survey agreed that installing backdoors would increase the frequency of security breaches by bad actors in the future.

The largest proportion of data breach costs is associated with compensations companies must pay to affected users, as well as the damage to a firm's reputation. Costs are related to the size of the data breach but also to the type of data exfiltrated, which can be categorized in a number of ways: PII (Personally Identifying Information), PHI (Protected Health Information), and PCI (Payment Card Industry). PHI is extremely sensitive as it is considered highly protected and private data. PCI is potentially the most disruptive data when stolen because it concerns financial credentials and can trigger a chain of extortion.

On average, the surveyed companies experienced 1 cybersecurity breach every four years. The median cost incurred due to the breach was reported as $100,001 to $499,999 in direct financial losses as a result of these malicious attacks.

But the indirect costs associated with weakened security infrastructure are likely to be even more profound. This is because the real value of encryption is in securing digital services and providing the basis of trust.

Research shows that the growing prominence of data breaches, and the development of laws and regulations to protect data privacy, has made security a key priority for consumers across the Five Eyes.[74]

- In Australia, 43% of consumers claim they would stop spending with a business for several months in the immediate aftermath of a security breach, and 43% of consumers claim they would never return to a business post-breach.
- In Canada, 58% of consumers claim they would stop spending with a business for several months in the immediate aftermath of a security breach, and a fifth of consumers claim they would never return to a business post-breach.
- In the UK, 44% of consumers claim they would stop spending with a business for several months in the immediate aftermath of a security breach, and 41% of consumers claim they would never return to a business post-breach.
- In the US, 83% of consumers claim they would stop spending with a business for several months in the immediate aftermath of a security breach, and over a fifth (21%) of consumers claim they would never return to a business post-breach.

From this perspective, weakening encryption is likely to impose costs on securing data, and pose a threat to “trust” in digital products and services, including trust in using the Internet and other data networks for e-commerce, which will increasingly include the entire economy. Increased compliance and security costs (69%), legal and remediation costs (46%), and damage to trust, reputation, and brand (42%) were highlighted as the biggest threats to SMEs from mandated encryption backdoors.

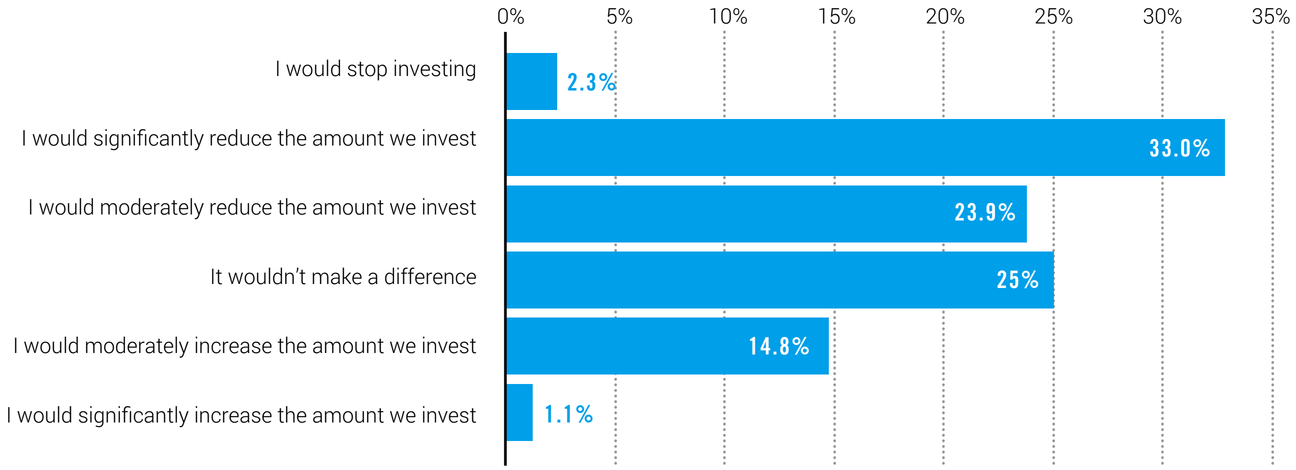
In the simplest economic analysis, the increased cost of providing “trusted” services will raise the costs of supply and decrease end-users’ willingness to pay. This would suggest an upward shift in aggregate supply and a downward shift in aggregate demand, resulting in a new higher equilibrium price at a lower level of aggregate demand. Prices would be higher and aggregate demand would be lower, producing what economists refer to as a "deadweight loss" associated with encryption backdoors.

One way to think about weakening encryption is to consider what the economic impact of reduced trust in cybersecurity might be for the aggregate economy. Reduced trust would lead to reduced demand for and activity in the digital economy, which would also reduce tech-driven productivity, growth, and innovation. A good example of this was Zurich Insurance Group's study in 2015,[75] which used a macroeconomic model to forecast the impact of different levels of trust in the internet on global economic growth.

Under a high-trust scenario, e-commerce was not threatened by cybercrime and the economic growth is faster, whereas under a worst-case scenario, cybercrime damages trust in online economic activity that e-commerce grows much more slowly. The base case is somewhere in between. This study pointed to a potential gap between the best- and worst-case forecasts of $USD 120 trillion, accounting for a 6% swing in cumulative global GDP, which demonstrates the serious threat this poses to economic growth.

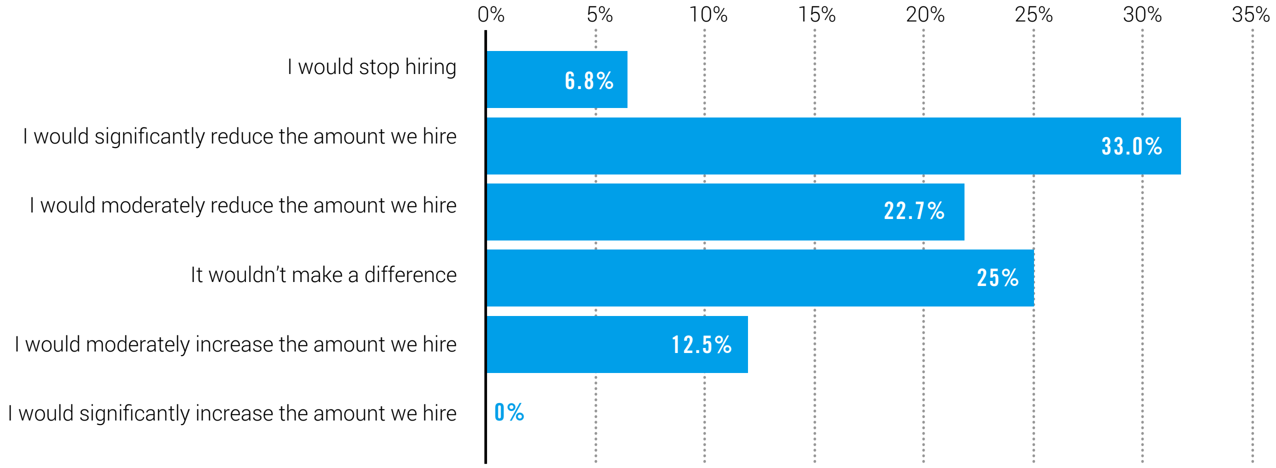
The slower growth is due to the joint effects of reduced demand to engage in online commerce and the resulting reduction in incentives by supply-side firms to invest in providing the capacity to support slower demand growth. When surveyed, 58% of business leaders reported that the proposed and enacted encryption regulations would negatively impact their investment decisions, and 62% reported that they would reduce or stop hiring.

## FIGURE 3: WHAT EFFECT WOULD A SIGNIFICANT WEAKENING OF DOMESTIC ENCRYPTION STANDARDS HAVE ON YOUR FUTURE INVESTMENT PLANS?



*Source: Beresford Research*

### FIGURE 4: WHAT EFFECT WOULD A SIGNIFICANT WEAKENING OF DOMESTIC ENCRYPTION STANDARDS HAVE ON YOUR FUTURE HIRING PLANS?



*Source: Beresford Research*

When the sample is restricted to countries with enacted encryption regulations — the United Kingdom, Australia, and New Zealand — a majority of the business leaders surveyed in those three countries report that weakening encryption standards will cause them to reduce hiring and investment.

To bring this to life, it is estimated that digital activity contributes $AU 426 billion ($USD 282 billion) to the Australian economy and generates $AU 1 trillion in gross economic output, supporting 1 in 6 jobs.[76] In the UK, digital services contribute £GBP 330bn ($USD 424 billion) to the economy, employ 5.2 million people, and support 1 in 8 jobs.[77] New Zealand has a much smaller digital economy that contributes $NZ 55 billion ($USD 34 billion), employing just under 44,000 thousand people, and accounts for 1 in 50 jobs.

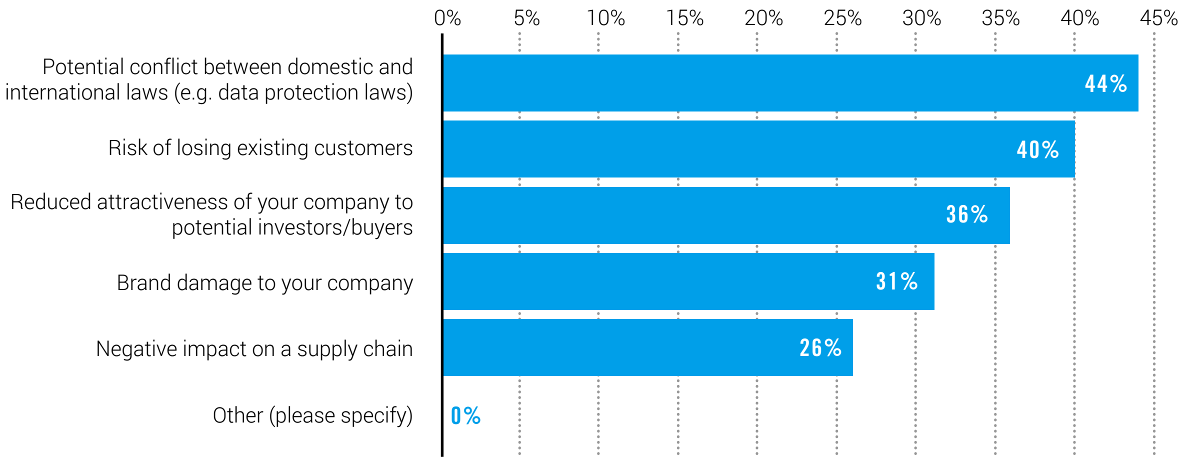
It is also feasible that there would be regional or sector-specific effects resulting from asymmetric threats to trust. If one country unilaterally implemented encryption backdoors, their tech sector could be expected to suffer a greater adverse shock associated with weakening encryption in the near term, with less trust in their products and services than the tech sectors in other countries that are not directly impacted. This would adversely impact their international competitiveness, and a majority of respondents in our survey (52%) indicated that weakening encryption standards would hurt their standing in global markets.

There are a number of reasons to anticipate why this could lead to an adverse impact on sales. For example, in July 2020, the European Court of Justice invalidated a negotiated workaround (Privacy Shield) that enabled US and European businesses to exchange customer data in a way that did not violate data privacy regulations. This situation forced companies to either cease their transatlantic data exchanges or increase their privacy measures, since any business that exports to the European market must comply with EU regulations.

Weakening encryption, therefore, is extremely likely to restrict companies' ability to export products and exchange data with their European counterparts. Making matters worse, the EU's GDPR is the global standard for privacy regulations around the world. This means that moves to weaken encryption could cause even further disruptions in data flows. The breakdown of these exchanges would have a disastrous impact on digital commerce.

Indeed, the most common concern shared by the surveyed SMEs (44%) was that mandated encryption backdoors will create a conflict between various different data protection laws around the world, such that the implementation of backdoors in one country might run afoul with stringent privacy laws in another. SMEs also reported that external perception — by investors and consumers alike — was a top concern.

## FIGURE 5: IF YOUR GOVERNMENT DECIDED TO IMPLEMENT "BACKDOORS" TO ENCRYPTION PRODUCTS AND SERVICES, WHICH OF THE FOLLOWING WOULD BE YOUR BIGGEST CONCERNS?



*Source: Beresford Research*

At the firm level, one might also anticipate that encryption regulations could result in a variety of direct and indirect effects. For example, the reduction in aggregate demand for a firm's products due to the reduction in market trust would shrink the pie for all firms. Additionally, the extent to which a firm suffered an even greater loss of trust might reduce that firm's market share of the lower aggregate demand. The effects of reduced data security might range from minor (e.g., the loss of a few sales for a few products) to major (e.g., the existential threat to a firm's future business if backdoors lead market participants to distrust the firm's commitment to transparency and securing customer data).

All other things being equal, a better brand image is associated with higher sales over time and, hence, a higher market value. Anything that threatens the relative perception of trust in a company can damage its brand and, hence, its sales prospects and business value. Taking these factors together, 48% of the small business leaders we surveyed believed that encryption backdoors would increase the perception of their product being less secure and trustworthy, damage their brand, and increase the risk of losing customers.

As we have already noted, the mandating of encryption backdoors would increase regulatory uncertainty. Increased technical, market, or regulatory uncertainty increases the riskiness of irreversible investments, which can delay or deter such investments. Measuring the impact of business uncertainty is difficult in general, but the only two quantitative studies conducted by the National Institute of Standards and Technology (NIST), in 2001 and 2018, provide an indication of the regulatory uncertainty associated with encryption technology.

In the 2001 NIST Encryption Impact Study,  the researchers sought to estimate the economic contribution that NIST's Data Encryption Standard (DES) added to the U.S. economy. They concluded that NIST's efforts accelerated the adoption of DES by several years, resulting in net benefits of between $USD 345 million and $USD 1.2 billion associated with lower costs for managing third-party bank data.

The follow-on study looked at the economic impact of the Advanced Encryption Standard (AES), which NIST also promoted the private sector to adopt.[78] The later study relied on a survey-based approach to derive estimates of how AES helped reduce the costs of firms active in deploying encryption technologies because of the existence of a federal standard. It estimated that the internal rate of return on NIST's investment in promoting AES was 81%, significantly more than NIST's 7% cost of capital, and the aggregate net benefits to the economy exceeded $USD 250 billion once all spillover effects were factored.

At the same time, analysts estimated the adverse impact on US companies from the Snowden revelations ranged from $35 billion to $180 billion in lost revenue.  Given the complex supply chain of encrypted services, the cascading effect from a loss in trust of the security of US companies caused major disruption across industries and regions. Cisco sales of routers dropped by 10%, and Amazon and Google had to cut their cloud prices by 51% to 53% as businesses sought non-US based providers.

Both of these studies show that a small investment in accelerating the deployment of encryption capabilities results in outsized gains to the economy. It also provides evidence that weakening said encryption would have a large adverse impact. What is clear is that any move to weaken encryption would result in significant economic self-harm to the tune of multiple billions of dollars.

We believe this is an important contribution to the debate around encryption regulation. Previously, much of the discussion has centered around large tech companies and consumer privacy. The results of this survey expand the debate to include the considerations of SMEs, an under-considered stakeholder in this discussion. As SMEs are often the largest employers in each country, we hope that these results will be a valuable contribution to the pool of considerations lawmakers reference as encryption regulations continue to develop.

At the same time, analysts estimated the adverse impact on US companies from the Snowden revelations ranged from $35 billion to $180 billion in lost revenue.  Given the complex supply chain of encrypted services, the cascading effect from a loss in trust of the security of US companies caused major disruption across industries and

regions. Cisco sales of routers dropped by 10%, and Amazon and Google had to cut their cloud prices by 51% to 53% as businesses sought non-US based providers

Both of these studies show that a small investment in accelerating the deployment of encryption capabilities results in outsized gains to the economy. It also provides evidence that weakening said encryption would have a large adverse impact. What is clear is that any move to weaken encryption would result in significant economic self-harm to the tune of multiple billions of dollars.

We believe this is an important contribution to the debate around encryption regulation. Previously, much of the discussion has centered around large tech companies and consumer privacy. The results of this survey expand the debate to include the considerations of SMEs, an under-considered stakeholder in this discussion. As SMEs are often the largest employers in each country, we hope that these results will be a valuable contribution to the pool of considerations lawmakers reference as encryption regulations continue to develop.

## RECOMMENDATIONS

The encryption debate is fraught with complexities and challenges, with governments and LEIAs seeking simple solutions to national security and public safety issues. But weakening encryption provides the illusion of protection while actually crippling the economy. We believe the safety of children and the public is absolutely paramount, but there are effective ways to combat crime without jeopardizing the privacy and security of every other public and private sector organization and individual.

Encryption workarounds are fraught with technical and policy challenges that would make them difficult, if not impossible, to deploy safely. We firmly believe that there are ways to protect the public and children's safety without chipping away the security that protects the entire digital economy and everyone who uses it.

But to achieve this, we must move away from overly simplistic propositions, and focus on the incremental steps that can enhance privacy and security and safeguard our communities. There is a lot more mutual interest between tech companies and law enforcement than the media likes to portray.

### Recommendation 1: Provide law enforcement with the necessary training to carry out their duties in the digital age.

Assumptions that encryption backdoors will provide a silver bullet to investigating child sexual abuse and terrorism, ignore the plethora of tools that LEIAs already have at their disposal to investigate online crimes and circumvent.

The proliferation of data across the digital economy has actually facilitated a "golden age" for intelligence and evidence gathering. Techniques that utilize metadata can uncover an individual's identity, even if the content is encrypted. While "lawful hacking" tools can already break encryption and enable the plaintext to be read. These have proved successful in countless high-profile cases, such as Operation Pacifier in 2015 which uncovered the identities of a global child abuse ring on the Dark Web.

But in order to use these techniques, law enforcement officials need to learn where to look for communication information. Currently, personnel are ill-equipped, and many do not actually know how to make basic requests to companies for data that they need to investigate crimes in general, not just computer-enabled crimes.[80] This knowledge and skills gap has real-world implications and contributes to unrealistic expectations about how various technologies work and how effective different forms of digital evidence can be. Without addressing this, we should expect constant encroachment by law enforcement to access more and more personal data over our lifetimes.

As an immediate step, governments should provide funding for digital forensics and evidence training for all law enforcement officials. In the US, the National Computer Forensics Institute (NCFI) acts as a coordinating hub for criminal intelligence and federal training for cyber-related investigations and digital forensics. While forensics training could help law enforcement at every level of society, few proposals to fight CSAM or other public threats include this basic, core training for modern detectives. Similar organizations and training programs would improve public safety in every Five Eyes country that is struggling to investigate criminal activity.

By properly funding training centers and various initiatives around a collection of digital evidence, law enforcement at all levels, not just the security and intelligence agencies, will be better equipped to investigate these incidents without having to rely on encryption backdoors that may lead to other challenges.

### Recommendation 2: Work collaboratively with tech companies to ensure illegal activity is minimized.

Technology companies do not want illegal content on their platforms and expend considerable resources to prevent it. Trust is of vital importance to the digital economy, and in scarce supply, which is why platforms have worked hard to prevent the spread of CSAM and other illegal content — it safeguards their users and builds trust in their services. It is much more of an existential issue than a matter of regulatory compliance.

In 2022, 230 technology companies across the globe were deploying tools and technology to detect CSAM, a 21% increase since 2020. This has significantly improved the joint mission to fight against CSAM and has made the fight against the abuse of children more effective.[81] Prima facie, an increase sounds worrying, but it is actually a good indicator that platforms are getting better at detecting CSAM. Thorn, a company that works with law enforcement and develops child safety technology, has asserted that “it shows that companies are getting better at proactively detecting, removing, and reporting abuse content”.[82] The uptick in detection has meant that more reports are being filed and more CSAM hashes created, which has significantly increased the evidence base to arrest and convict perpetrators.

At the user level, tech companies have installed countless controls and reporting mechanisms by default, to make illegal content easier to identify and remove, as well as improving parental discretion and oversight of their child’s online activity. In fact, Apple’s proactive initiative to try and develop client-side scanning technology to detect CSAM stored in iCloud, and automatically flag it to law enforcement, shows just how much good faith exists. The company pushed the technical limits of encryption to the extreme, but found it amounted to a security backdoor. These systems could have also been repurposed for surveillance and censorship, and requests to technology companies from around the world have proven the desire to target political dissidents, religious minorities, and others.

Yet, tech companies are still caught in the middle of government requests to ensure their users' data is secure, as well as providing LEIAs with access to more data. Governments should not be asking private companies to deputize as law enforcement.[84] It not only establishes a democratic-deficit, it also blurs important lines and puts employees in a position where there will inherently be conflicts of interest between their duties to users, to their business, and to governments. If this contributed to harm or a violation of rights, who would be held accountable? How would this semi-private law enforcement arrangement be justified to taxpayers?

Governments must work collaboratively with the private sector, instead of running ahead with ill-thought legislation, and shouting past technologists when they say that the thing they want is technically impossible to deliver. A more fruitful partnership could encourage more platforms to implement detection tools, provide better user controls, and develop the next generation of privacy-enhancing solutions. This would deepen the evidence base for law enforcement and harness the innovative power of the private sector to help fight societal harms — strengthening the joint mission more effectively.

### Recommendation 3: Target interventions at the source of the disease not the symptom

While technology platforms need to deliver on their responsibilities, given their undoubted scope and global reach, they alone cannot fix deep-seated social problems. Similarly, online harms can not be an excuse for governments to piggyback on the reach of tech companies to do things that would not be compatible with democratic accountability offline.

Some harms need offline interventions or can be better addressed offline; for example, tackling the abuse of children or vulnerable people requires the involvement of local police, social services, and schools, which all need to have a legal framework enabling them to act and adequate resources with which to do so. There are a number of legislative efforts at various stages across the Five Eyes, so it would be opportune to target legislation in a way that stamps out illegal content at its source — the individual.

Legislation should include centralized mechanisms that coordinate efforts to prevent, investigate, prosecute, and treat victims of child exploitation, as well as increased funding for law enforcement activities that prevent child exploitation and create standardized reporting requirements for online services to use when notifying authorities of potential crimes. These steps would help law enforcement agencies and online services work together more efficiently to find perpetrators and shield children from harm.

Resources should also be prioritized for law enforcement's ability to tackle cybercrime. This would provide a strong start and pivot the focus towards improved prosecution of online criminals. For decades, the number of police on the streets has been prioritized over other, more intelligence-focused, functions (e.g., the UK's National Crime Agency) for vote-winning reasons. Internet crime has grown rapidly over the last decade, and, for example, cyberspace is now the favorite realm for fraudsters.[85] Platforms should also be encouraged to help develop a base of evidence, provide early warnings of new criminal activity, and promote best practice.

Governments should seek to incentivize reporting and build stronger public-private partnerships with online services to tackle the worst the Internet has to offer. The focus of child safety legislation and law enforcement legislation should be to provide more resources to the nation's police, and law enforcement agencies, to tackle cybercrime. Providing authorities and regulators with the resources to work with online services would improve how they report illegal activity, which would significantly increase the ability of law enforcement to track, remove, and prosecute cybercrime.

## CONCLUSION

Encryption plays a critical role in enabling the digital economy to thrive by ensuring data privacy and security, which is integral to consumer trust in e-commerce, financial transactions, digital health, e-learning, secure information storage, and secure private communications, and by assuring our civil liberties, such as privacy, freedom of speech, and freedom of association.

Exceptional access has been touted as the only way to solve CSAM and other crimes but it's a distraction — crime is the real problem — not encryption or technology. It is clear that weakening encryption would jeopardize the security, privacy, and vital social interests of every business, organization, and individual. As our research shows, there is no universal solution, no silver bullet, and no magic wand capable of weakening encryption without inflicting tremendous economic self-harm in the *multiple billions of dollars.*

Other solutions and methods exist to support law enforcement's efforts online while also protecting the privacy of law-abiding citizens. These approaches have been advocated by the Center for Strategic and International Studies (CSIS) as well as the Carnegie Endowment for International Peace, Princeton University, and the University of Oxford. It is imperative to shift our focus towards gradual progress.

There is a common cause that unites both technology companies and law enforcement: preventing crimes from happening in the first place to protect children and the public. It is through this lens that policymakers must rethink the conversation, and accept that incremental progress is key to innovation.

## ABOUT THE AUTHORS

**Joel Gladwin** served as the Special Adviser to two Secretaries of State for Digital Culture Media & Sport (DCMS) in His Majesty's Government between May 2021 and September 2022. He worked on a number of tech policy issues including the Online Safety Act, artificial intelligence, tech regulation, competition & antitrust, as well as investment and skills policy. Prior to this, Joel was Head of Policy at the Startup Coalition, the industry body representing UK tech startups and scaleups. He is currently a strategic adviser to a number of technology companies in regulated sectors.

**Colin Mortimer** is a Director at the Progressive Policy Institute and a Board Member of New Democracy. Before joining PPI, Mortimer was a consultant at Bates White Economic Consulting and a research assistant at the University of Connecticut. Colin holds B.A. in Economics and Mathematics-Statistics from the University of Connecticut.

# References

1 Bhandari V, Bailey R, Rahman F. (2021) Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805980.

2 Dheri P, Cobey D. (2019) Lawful Access & Encryption in Canada: A Policy Framework Proposal, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470957.

3 Ibid.

4 Ibid.

5 Moraes T. (2020) Sparkling Lights in the Going Dark: European Data Protection Law Review, https://edpl.lexxion.eu/article/EDPL/2020/1/7.

6 Ibid.

7 Scott R. Ellis (2013) A Cryptography Primer, https://www.sciencedirect.com/science/article/abs/pii/B978012803843700003X.

8 Rozenshtein AZ. (2018) Surveillance Intermediaries. https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf.

9 Harkens A. (2016) "Rear Window Ethics" and Discrimination: The Darker Side of Big Data, https://research.birmingham.ac.uk/en/publications/rear-window-ethics-and-discrimination-the-darker-side-of-big-data.

10 See NIST (2015, 2018), discussed further below.

11 Cebr (2022) Digital Trust Index, https://www.callsign.com/digital-trust-index.

12 Van Daalen O.L. (2023) The right to encryption: Privacy as preventing unlawful access, https://www.sciencedirect.com/science/article/pii/S0267364923000146.

13 Rozenshtein AZ. (2018) Surveillance Intermediaries, https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf.

14 Gill L, Israel T, Parsons C. (2018) Shining a Light on the Encryption Debate: A Canadian Field Guide, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.

15 Ropek L. (2023) The Short Life and Humiliating Death of the Clipper Chip, https://gizmodo.com/life-and-death-of-clipper-chip-encryption-backdoors-att-1850177832.

16 Thompson AW, Park C. (2020) Privacy's Best Friend, https://www.newamerica.org/oti/reports/privacys-best-friend/.

17 Gill L, Israel T, Parsons C. (2018) Shining a Light on the Encryption Debate: A Canadian Field Guide, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.

18 Ibid.

19 Zwillgen PLC (2016) In re Order Requiring Apple Inc. to Assist in the Execution of a Search Warrant Issued by the Court, No. 15-MC-1902, https://www.justsecurity.org/wp-content/uploads/2016/03/Apple-All-Writs-Apple-Requests-Received-Letter.pdf.

20 Portnoy E. (2019) Why Adding Client-Side Scanning Breaks End-To-End Encryption, https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning- breaks-end-end-encryption.

21 Muffett A. (2022) A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022, https://alecmuffett.com/article/16184

22 Apple (2021) Expanded Protections for Children, https://www.apple.com/child-safety/.

23 Ibid.

24 Internet Society (2020) Fact Sheet: Client Side Scanning—What It Is and Why It Threatens Trustworthy, Private Communications, https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

25 Nakashima E, Harris S. (2020) Elite CIA unit that developed hacking tools failed to secure its own systems, allowing massive leak, an internal report found, https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077_story.html.

26 Schneier B. (2020) Who Are the Shadow Brokers?, https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

27 Nash K, Castellanos S, Janofsky A. (2018) One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs, https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

28 Smith G. (2017) Back Doors, Black Boxes and #IPAct Technical Capability Regulations, http://www.cyberleagle.com/2017/05/back-doors-black-boxes-and-ipact.html.

29 UK Parliament (2023) Online Safety Act 2023, https://bills.parliament.uk/bills/3137.

30 Home Office (2023) Guidance: End-to-end Encryption and Child Safety, https://www.gov.uk/government/publications/end-to-end-encryption-and-child-safety/end-to-end-encryption-and-child-safety.

31 Manancourt V. (2023) U.K. Dials Up Fight With Meta Over Encryption, https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email.

32 Whittaker M, (2023) Standing Firm Against Threats To Private And Safe Communication, https://signal.org/blog/uk-online-safety-bill/.

33 Manancourt V. (2023) U.K. Dials Up Fight With Meta Over Encryption, https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email.

34 Saddle P. (2023) UK Urges Meta Not To Roll Out End-To-End Encryption On Messenger And Instagram, https://shorturl.at/ikmB8

35 Shah S. (2023) Messenger Will Finally Get End-To-End Encryption By The End Of The Year, https://www.standard.co.uk/news/tech/messenger-end-to-end-encryption-b1102746.html.

36 Milmo D., (2023) Meta Taskforce to Combat Trade of Child Sex Abuse Materials After Damning Report, https://www.theguardian.com/technology/2023/jun/07/meta-instagram-self-generated-child-sexual-abuse-materials.

37 Home Office (2023) Investigatory Powers (Amendment) Bill: Overview, https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-overview.

38 Australian Department of Home Affairs (2018) The Assistance and Access Act 2018, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption.

39 Parliament of Australia (2020) Parliamentary Joint Committee on Intelligence and Security - 07/08/2020 - Telecommunications

and Other Legislation Amendment (Assistance and Access) Act 2018, https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/30904d8b-7cfb-4ef0-99fb-.

40 Australian eSafety Commissioner (2023) Statement On End-To-End Encryption And Draft Industry Standards, https://www.esafety.gov.au/newsroom/media-releases/statement-on-end-to-end-encryption-and-draft-industry-standards#:~:text=eSafety%20is%20seeking%20feedback%20on,and%20pro%2Dterror%20material%20online.

41 eSafety Commissioner (2023) Discussion Paper: Draft Online Safety (Relevant Electronic Services – Class 1A and 1B Material) Industry Standard 2024, https://www.esafety.gov.au/sites/default/files/2023-11/Discussion-Paper-draft-Online-Safety-Standards-%28Class-1A-and-1B%29.pdf.

42 Gill, L. (2018). Law, Metaphor and the Encrypted Machine, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933269.

43 Koops BJ, & Kosta E. (2018). Looking for Some Light Through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities Against "Going Dark," https://doi.org/10.1016/j.clsr.2018.06.003.

44 Johnson A & Castro D. (2021) Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved, https://itif.org/publications/2021/02/22/overview-section-230-what-it- why-it-was-created-and-what-it-has-achieved/.

45 Gill L, Israel T, Parsons C. (2018) Shining a Light on the Encryption Debate: A Canadian Field Guide, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.

46 West, L & Forcese, C. (2020). Twisted into Knots: Canada's Challenges in Lawful Access to Encrypted Communications, https://doi.org/10.1177/1473779519891597.

47 Gill L, Israel T, Parsons C. (2018) Shining a Light on the Encryption Debate: A Canadian Field Guide, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf.

48 Cooper, S. (2018). An Analysis of New Zealand Intelligence and Security Agency Powers to Intercept Private Communications: Necessary and Proportionate?, http://www.nzlii.org/nz/journals/AukULawRw/2018/6.pdf.

49 Dizon, M et al. (2019). A Matter of Security, Privacy and Trust: A study of the principles and values of encryption in New Zealand, http://www.nzlii.org/nz/journals/NZLFRRp/2019/14.html.

50 Keith, B. (2020). Official Access To Encrypted Communications In New Zealand: Not More Powers But More Principle?, https://journals.sagepub.com/doi/10.1177/1473779520908293?icid=int.sj-full-text.similar-articles.5.

51 Department of Internal Affairs (2023) Safer Online Services and Media Platforms, https://www.dia.govt.nz/diawebsite.nsf/Files/online-content-regulation/$file/Safer-Online-Services-and-Media-Platforms-Discussion-Document-June-2023.pdf.

52 Deeks, A. (2020) The International Legal Dynamics of Encryption, https://papers.ssrn.com/abstract=3587438.

53 O'shea, L & Thomas, E. (2018) The Role of Encryption in Australia: A Memorandum, https://digitalrightswatch.org.au/wp-content/uploads/2018/01/Crypto-Australia-Memo.pdf.

54 Article 19 (2021) Russia Telegram Block Leads To Widespread Assault on Freedom of Expression Online, https://www.article19.org/resources/russia-telegram-block-leads-widespread-assault-freedom-expression-online/.

55 ISOC Switzerland Chapter (2021) Statement: ISOC Switzerland Chapter Concerned over Reports that EU Plans to Weaken Encryption, https://www.isoc.ch/statement-isoc-switzerland-chapter-concerned-over-reports-that-eu-plans-to-weaken-encryption/

56 McGarrity, N & Hardy K. (2020) Digital Surveillance and Access to Encrypted Communications in Australia, https://carnegieendowment.org/2021/03/31/encryption-debate-in-australia-2021-update-pub-84237#:~:text=In%202018%2C%20the%20heads%20of,gain%20access%20to%20encrypted%20communications

57 Carter, W & Daskal J. (2018) Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf.

58 Meineck S, Reuter, M (2022) EU-Kommission nimmt hohe Fehlerquoten bei Chatcontroller, https://netzpolitik.org/2022/geleakter-bericht-eu-kommission-nimmt-hohe-fehlerquoten-bei-chatkontrolle-in-kauf/.

59 BBC (2017) FBI Failed to Access 7,000 Encrypted Mobile Devices, https://www.bbc.co.uk/news/technology-41721354.

60 Nakashima N. (2018) Inspector General: FBI Didn't Fully Explore Whether It Could Hack a Terrorists iPhone Before Asking a Court to Order Apple to Unlock It, https://www.washingtonpost.com/world/national-security/inspector-general-fbi-didnt-fully-explore-whether-it-could-hack-a-terrorists-iphone-before-asking-court-to-order-apple-to-unlock-it/2018/03/27/b56a9dca-31cf-11e8-8abc-22a366b72f2d_story.html

61 Brandom R. (2016) The FBI Has Gotten No New Leads from the San Bernardino iPhone, https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads.

62 Bhandari V, Bailey R, Rahman F. (2021) Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805980.

63 Liguori C. (2020) Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1019&context=mtlr.

64 Herpig S. (2018) A Framework for Government Hacking in Criminal Investigations, https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf.

65 Ibid.

66 Voors MP. (2003) Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security At The Expense of the Economy?, https://www.repository.law.indiana.edu/fclj/vol55/iss2/7/.

67 Chertoff Group (2016) The Ground Truth About Encryption, https://cdn2.hubspot.net/hubfs/3821841/docs/238024-282765.groundtruth.pdf.

68 Article 19 (2021) Russia Telegram Block Leads to Widespread Assault on Freedom of Expression Online, https://www.article19.org/resources/russia-telegram-block-leads-widespread-assault-freedom-expression-online/.

69 Stepanovich, A & Karanicolas M. (2018) Why An Encryption Backdoor for Just the "Good Guys" Won't Work, https://www.justsecurity.org/53316/criminalize-security-criminals-secure/.

70 IBM (2022) Cost of a Data Breach Report 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ.

71 Deeks, A. (2020) The International Legal Dynamics of Encryption, https://papers.ssrn.com/abstract=3587438.

72 Ibid.

73 Bridgwater, A. (2016) Veritas: EU Data Protection Laws to Affect All Global Firms, https://www.forbes.com/sites/adrianbridgwater/2016/05/25/veritas-eu-data-protection-laws-to-affect-all-global-firms/?sh=4ac7d1d92171.

74 PCI Pal (2019) New Global Research Shows Poor Data Security Practices Have Serious Consequences for Businesses Worldwide, https://www.businesswire.com/news/home/20190917005012/en/New-Global-Research-Shows-Poor-Data-Security.

75 Zurich (2015) Risk Nexus: Overcome By Cyber Risks? Economic Benefits And Costs Of Alternate Cyber Futures, https://www.atlanticcouncil.org/wp-content/uploads/2015/09/risk-nexus-september-2015-overcome-by-cyber-risks.pdf.

76 AustCyber (2020) Australia's Digital Trust Report, https://www.austcyber.com/resource/digitaltrustreport2020.

77 CCIA & Public First (2024) State of the UK Digital Economy, https://ccianet.org/research/reports/uk-digital-economy/.

78 Leech, D & Scott, J. (2018) The Economic Impacts of the Advanced Encryption Standard, 1996-2017, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918355.

79 Boulton, C (2013) NSA's PRISM Could Cost IT Service Market $180 Billion, https://www.wsj.com/articles/BL-CIOB-2608

80 Carter, W & Daskal J. (2018) Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf.

81 The National Center for Missing & Exploited Children (2022) CyberTipline 2022 Report, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.

82 Thorn (2022) New Report Shows an Increased Effort by Tech Companies to Detect CSAM on the Internet, https://www.thorn.org/blog/new-report-shows-an-increased-effort-by-tech-companies-to-detect-csam-on-the-internet/.

83 Portnoy E. (2019) Why Adding Client-Side Scanning Breaks End-To-End Encryption. https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.

84 Wheeler T. (2023) There's A Cop In My Pocket: Policymakers Need to Stop Advocating Surveillance by Default, https://www.cfr.org/blog/theres-cop-my-pocket-policymakers-need-stop-advocating-surveillance-default.

85 Home Office (2023) World First Agreement To Tackle Online Fraud, https://www.gov.uk/government/news/world-first-agreement-to-tackle-online-fraud.

ppi

The Progressive Policy Institute is a catalyst for policy innovation and political reform based in Washington, D.C. Its mission is to create radically pragmatic ideas for moving America beyond ideological and partisan deadlock.

Founded in 1989, PPI started as the intellectual home of the New Democrats and earned a reputation as President Bill Clinton's "idea mill." Many of its mold-breaking ideas have been translated into public policy and law and have influenced international efforts to modernize progressive politics.

Today, PPI is developing fresh proposals for stimulating U.S. economic innovation and growth; equipping all Americans with the skills and assets that social mobility in the knowledge economy requires; modernizing an overly bureaucratic and centralized public sector; and defending liberal democracy in a dangerous world.

**PROGRESSIVE POLICY INSTITUTE**
1919 M Street NW,
Suite 300,
Washington, DC 20036

**Tel** 202.525.3926
**Fax** 202.525.3941

info@ppionline.org
progressivepolicy.org