Is E2EE a Shield or a Barrier? The Struggle over End-To-End Encryption in the U.S.

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Nurbol Lampert

March 27, 2025

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Nurbol Lampert

STS Advisor: Peter Norton

Introduction

End-to-end encryption (E2EE) has become a linchpin of modern cybersecurity. It scrambles data so thoroughly that not even the service providers can decipher user content without permission. Privacy advocates stress that robust encryption safeguards personal privacy, protects citizens from cyberattacks, and underpins trust in digital services (EFF, 2015). By contrast, law enforcement and intelligence agencies warn that E2EE hampers critical investigations by making evidence inaccessible – a concern often termed the "going dark" problem (FBI, 2020). Balancing individual privacy and public safety has thus become an intricate challenge (ACLU, 2023).

As digital communications proliferate, encryption now shields vast troves of personal and business data from hackers and hostile actors. Yet the same technology can frustrate efforts to investigate serious crimes like terrorism, child exploitation, and organized cyberattacks (Law Enforcement Coalition, 2018). Law enforcement agencies demand mandatory "backdoors" in encrypted systems, but tech companies and privacy advocates contest such demands, citing civil liberties and cybersecurity (CDT, 2017). Encryption inherently redistributes power: it diminishes state surveillance capabilities and amplifies individual autonomy by placing control of information in users' hands (Abelson et al., 2015). This power shift clashes with law enforcement's duty to protect the public, fueling high-profile confrontations and proposals to regulate encryption. In 2020, for example, when Congress introduced the EARN IT Act to curb online child abuse, critics condemned the bill as a veiled attempt to weaken encryption (U.S. Congress, 2020). Apple and WhatsApp have refused to implement "exceptional access" systems, insisting they would undermine security for all users (Apple Inc., 2016; Cathcart, 2021). They warn that criminals or authoritarian governments can exploit backdoors as easily as investigators.

Review of Research

Scholars have described the encryption debate as highly polarized while noting that its framing as privacy versus security often overlooks deeper complexities. Herath and Dawda (2022) characterize the policy discourse as locked in a zero-sum mentality, calling for more nuanced solutions that transcend this false dichotomy (Herath and Dawda, 2022). Green and Smith (2016) observe that the so-called "crypto wars" of the 1990s – when the U.S. government first tried to mandate escrowed encryption keys – never truly ended, because the underlying tension between state access and individual privacy persists in new forms (Green and Smith, 2016). Historical research shows that previous attempts to restrict encryption (e.g., the Clipper Chip initiative) failed under intense opposition from technologists, civil liberties organizations, and portions of industry.

Empirical evidence on encryption's real-world impact remains limited but is gradually emerging. Hartel and van Wegberg (2023), for instance, examined Dutch criminal cases and concluded that strong encryption did not automatically thwart prosecutions, implying some adaptability on the part of law enforcement (Hartel and van Wegberg, 2023). However, they also emphasized the challenge of tracking cases that never advance due to inaccessible evidence – suggesting that any quantitative measures of encryption's impact may under-represent its actual effects. Landau (2021) likewise argues that the "going dark" narrative can be misleading if it fails to account for the many investigative tools and techniques, such as metadata analysis or lawful hacking, that remain available even when data is encrypted end-to-end (Landau, 2021).

Technical experts generally concur that creating any form of "exceptional access" poses grave risks to overall cybersecurity. Abelson et al. (2015) famously warned that mandating

backdoors ("keys under doormats") for the government undermines the security of all users, since no reliable mechanism exists to distinguish "legitimate" from illegitimate use of that access (Abelson et al., 2015). Rogers (2003) adds a sociotechnical perspective, positing that encryption's diffusion is shaped as much by public attitudes and institutional trust as by technical feasibility (Rogers, 2003). Researchers like Mohapatra (2020) highlight the authoritarian potential of backdoors, noting that repressive regimes can exploit any universal-access mechanism to suppress dissent (Mohapatra, 2020). Nye (2011) similarly observes that encryption alters the distribution of power in digital systems, transferring control from states to private actors (Nye, 2011). These studies collectively indicate that the conflict over encryption arises not purely from engineering constraints, but from competing social priorities and the evolving dynamics of trust and authority in networked societies.

The Power Dynamics of Encryption

The tug-of-war over encryption can be understood as a struggle over power in the digital realm. Encryption alters power dynamics by shifting who can control and access information. On one side, individuals and companies gain power: strong E2EE lets them safeguard data against unauthorized access, thereby limiting government and corporate surveillance. Civil liberties organizations argue that redistribution of power advances democratic ideals, enabling free speech and dissent without fear of indiscriminate monitoring (ACLU, 2023). On the other side, law enforcement officials contend that if criminals can "go dark" behind impenetrable encryption, it creates zones where the law cannot reach, undermining society's ability to protect itself (FBI, 2020). As Attorney General William Barr put it, "making our virtual world more secure [with

encryption] should not come at the expense of wholly precluding society's ability to defend itself against criminal threats" (DOJ, 2019).

These clashing perspectives are vividly illustrated in the rhetoric each side uses. A joint statement by an international law enforcement coalition warned that end-to-end encryption which "wholly precludes any legal access to content" creates severe risks to public safety, calling on tech companies to find solutions that enable lawful access when necessary (Law Enforcement Coalition, 2018). By contrast, tech leaders assert that deliberately weakening encryption, even slightly, would fatally erode user trust and security. Apple's CEO Tim Cook famously refused an FBI demand to unlock an iPhone, writing that "the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create" – namely a backdoor into the iPhone's encryption (Apple Inc., 2016). In Apple's view, creating that capability for one device would amount to creating a master key that could open millions of devices if it fell into the wrong hands. This standoff encapsulates the power struggle: government agencies seek the authority to compel access in extraordinary cases, while tech firms and privacy advocates resist, fearing the broader consequences of setting such a precedent.

Case Study: Apple vs. FBI in the San Bernardino Investigation

A defining episode in the debate unfolded after a 2015 terrorist attack in San Bernardino, California, when the FBI recovered an iPhone belonging to one of the attackers. Investigators obtained a court order under an 18th-century law (the All Writs Act) demanding that Apple create software to bypass the phone's encryption – essentially a request for a bespoke backdoor. Apple very publicly refused. In a letter to customers, CEO Tim Cook argued that the government was asking Apple to weaken its product's security in a way that would "make everyone less safe"

and set a dangerous precedent (Apple Inc., 2016). The clash escalated into a major public debate over whether companies can be compelled to undermine their own security features. Ultimately, the FBI found a third-party vendor to hack into the device without Apple's help, and the legal case was dropped.

Even though the immediate crisis was resolved, the implications were far-reaching. The Apple–FBI standoff brought the encryption issue into the national spotlight. FBI Director James Comey and others cited the case as evidence of the "going dark" problem, arguing to Congress that new tools or laws were needed so criminals could not evade detection via encryption (FBI, 2020). Apple's defiance, on the other hand, reinforced the tech industry's resolve to protect user privacy. Despite extensive congressional hearings and discussions in 2016–2017, no legislation was passed to force decryption, in part because consensus proved elusive. The San Bernardino case showed that while law enforcement can sometimes find workarounds (like hiring hackers), Silicon Valley is willing to fight vigorously against mandated vulnerabilities. It set the stage for ongoing legislative battles seeking a broader solution to the encryption challenge.

Legislative Battles: The EARN IT Act and Other Proposals

In the wake of incidents like the Apple–FBI clash, U.S. lawmakers have floated various bills to reconcile encryption with law enforcement needs. The most notable attempt has been the EARN IT Act of 2020, a bipartisan bill ostensibly aimed at curbing online child sexual abuse. EARN IT threatened to withdraw certain legal protections from online platforms unless they complied with government-approved best practices to find and remove child abuse material. While the bill did not explicitly mandate encryption backdoors, critics argued that it would pressure companies to weaken or surveil encrypted services as part of those "best practices"

(U.S. Congress, 2020; ACLU, 2023). Digital rights groups warned that EARN IT effectively put encryption on trial, and many tech companies also voiced opposition. Amid the controversy, the 2020 version of the act stalled. Revised versions have been reintroduced in subsequent years, reflecting a continued legislative push to address the "going dark" issue indirectly.

Other proposals have taken a more direct approach. For instance, the Lawful Access to Encrypted Data Act (2020) would have outright required device manufacturers and service providers to assist law enforcement in decrypting data upon court order. That bill, like EARN IT, faced staunch resistance from the tech industry and privacy advocates and did not advance. To date, no U.S. law compels companies to introduce decryption mechanisms, and debates in Congress remain unresolved.

International developments have added momentum and complexity to U.S. discussions. In 2018 Australia enacted a law compelling technology companies to provide law enforcement access to encrypted communications when required, effectively authorizing government-mandated points of access. Officials in the U.S. (and elsewhere) often cite Australia's example to argue that lawful access requirements can coexist with tech innovation (DOJ, 2019). The European Union has also considered regulations that would require scanning of encrypted messages for illicit content, which observers note could undermine E2EE. These moves abroad increase pressure on U.S. policymakers by showing a willingness among allies to legislate in this space. However, they also validate civil liberties groups' fears of a global erosion of secure communications if one nation's policy creates a precedent. So far, American legislators have been more cautious – perhaps due to the formidable coalition of privacy advocates, cybersecurity experts, and companies united against any law that would weaken encryption for all users.

Industry Responses and the Client-Side Scanning Debate

Tech companies have found themselves under pressure to assist with investigations without undermining their products' security. One of the most controversial experiments was Apple's 2021 proposal for client-side scanning on iPhones. Apple announced plans to update iOS so that a user's photos would be automatically scanned on the device for known child sexual abuse material (CSAM) before being uploaded to iCloud (ACLU, 2023). The idea was to intercept illegal content even within an encrypted ecosystem, thereby aiding law enforcement against child predators. However, privacy advocates and security experts quickly criticized the plan. They argued that even this carefully designed system amounted to installing a surveillance mechanism on every iPhone, fundamentally compromising the promise of E2EE (EFF, 2019). If Apple could scan for one type of prohibited content, they warned, governments could compel it to scan for others (political dissent, etc.), turning the phone into a general monitoring tool. In response to the backlash – summed up by the slogan "Don't scan my phone" – Apple indefinitely postponed and eventually cancelled the CSAM scanning feature. Instead, by late 2022 Apple shifted course and actually strengthened user privacy protections, extending end-to-end encryption to iCloud backups that were previously not fully encrypted.

The client-side scanning saga illustrated that even well-intentioned compromises face immense challenges in this domain. If a scanning system is effective enough to catch criminals, it inherently intrudes on user privacy; if it is constrained to preserve privacy, its utility to law enforcement diminishes. In the aftermath, major tech firms have largely doubled down on providing robust encryption across their services. Companies continue to cooperate with law enforcement through less intrusive means – for example, complying with lawful requests for

metadata or providing cloud data that is not end-to-end encrypted – but they remain reluctant to build in any universal bypass. Their stance, reinforced by user expectations and global competition, is that the core encryption protecting user communications should remain off-limits, and that investigative solutions must be found that do not undermine the security of everyone's data.

Apple's Withdrawal of Advanced Data Protection in the UK

Recent events have highlighted how international law can undermine end-to-end encryption through direct legal pressure. In February 2025, Apple disabled its Advanced Data Protection (ADP) feature in the United Kingdom, citing demands from UK authorities under the Investigatory Powers Act (IPA). ADP provided end-to-end encryption for iCloud backups, ensuring that even Apple could not unlock users' cloud-stored data (AppleInsider, 2025; The Guardian, 2025). By turning off ADP for British users, Apple complied with a technical notice requiring that providers maintain the capability to read data when served a warrant.

Observers view this as a significant concession, as Apple had promoted ADP as a cornerstone of user privacy. Privacy advocates warned that government pressure to access any user's data, without building a targeted solution, invites "a backdoor by another name" (The Verge, 2025a). Apple's reluctant move illustrates how a single national legal regime can force global tech companies to scale back encryption in one jurisdiction, creating a fragmented security landscape. While Apple did not install a new backdoor, critics note that British iCloud data is no longer fully encrypted at rest, making it accessible to Apple and therefore subject to search by law enforcement.

The UK's updated Investigatory Powers Act, combined with its Online Safety legislation, grants authorities broad powers to demand encryption workarounds. Companies receiving such notices often must keep them secret, raising questions about transparency and accountability (The Verge, 2025b). Apple's withdrawal of ADP thus emerged publicly only after media reports, prompting swift condemnation from civil liberties organizations. Security analysts worry that other countries – some with authoritarian leanings – may follow the UK's approach (Proton, 2025). Platform leaders like WhatsApp and Signal have already threatened to leave the UK rather than weaken encryption, suggesting that Apple's compromise sets a dangerous precedent. The episode underscores a sobering reality: government powers to mandate decryption or block advanced encryption features can circumvent the broader U.S. debate, compelling companies to adopt weaker security in certain markets.

Counterarguments and Ethical Dimensions

At its core, the encryption controversy raises a moral dilemma over whether privacy or public safety should prevail when they appear to clash. Privacy advocates assert that encryption is indispensable for freedom of expression and protection against unjust surveillance (ACLU, 2023). Government overreach remains a live concern: even democratic states have historically abused surveillance powers, and authoritarian regimes can misuse any backdoor to suppress dissent. By contrast, law enforcement and many in the public consider it morally necessary to protect victims, arguing that encryption effectively conceals serious crimes if no lawful mechanism exists for investigators to access vital data. Cases involving terrorism or child exploitation intensify the moral imperative for decryption, even if partial.

Weakening encryption, however, poses new vulnerabilities. Hackers, foreign spies, or rogue insiders could exploit a universal key intended for authorized investigations. Civil libertarians warn that such systemic flaws endanger everyone's privacy. The ethical tension is that absolute privacy may impede justice in certain cases, while universal accessibility jeopardizes the broader security that encryption provides. Most specialists agree that neither extreme – fully warrant-proof encryption nor universal backdoors – resolves the dilemma, thus driving a search for targeted and transparent alternatives.

Conclusion

Entrenched differences between law enforcement, technology companies, and civil liberties organizations have yielded a prolonged standoff over end-to-end encryption in the United States. Public officials assert that criminals abuse encryption to conceal evidence of terrorism, child abuse, and other serious crimes, and that no responsible society should allow technology to become "warrant-proof" (DOJ, 2019). Opponents respond that a master key for law enforcement, even if legally restricted, would ultimately place everyone's data at risk, since hacking groups or repressive regimes could exploit the same vulnerabilities. Tech companies highlight the global demand for secure products, while civil liberties groups recall historical abuses of government surveillance to emphasize the fragility of privacy rights.

Recurring controversies – including the Apple – FBI case, the EARN IT Act, debates over client-side scanning, and now Apple's withdrawal of Advanced Data Protection in the UK – demonstrate how all sides refuse to concede on core principles. Recent UK developments reveal how national laws can override corporate encryption policies and force providers to reduce security features. Observers question whether such forced accommodations will embolden

additional governments to follow suit, potentially fragmenting encryption standards worldwide. Law enforcement prioritizes the imperative to protect victims and investigate crimes, whereas tech leaders and privacy advocates seek to preserve digital security for law-abiding users. Industry also argues that strong encryption engenders trust and economic viability on a global scale. Legal attempts to compel decryption have stalled, leaving agencies to rely on alternative tactics like targeted hacking. Scholars studying encryption see little prospect of a consensus, given that proposed solutions often erode security for everyone or restrict legitimate criminal investigations too severely.

A more durable arrangement may require new investigative models that do not rely on universal backdoors. Officials could pursue narrower techniques with firm judicial oversight – focusing on suspects through proven hacking tools or metadata. Companies might continue refining ways to detect harmful activity in unencrypted contexts without scanning all user data. Civil society will likely retain a critical watchdog role, insisting that surveillance powers remain accountable. This tension in the encryption domain reflects a broader challenge for democratic societies: how to reconcile individual rights and collective security when advances in technology shift power away from institutions and toward private hands. The conflict over E2EE has forced a reckoning with the meaning of public safety and privacy in the digital era, and the outcome will shape the future of American civil liberties, technological innovation, and the rule of law.

References

Abelson, Anderson, Bellovin, Benaloh, Blaze, Diffie, and Weitzner (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1), 69–79.

ACLU (2023, Oct. 20). American Civil Liberties Union. The Vital Role of End-to-End Encryption. www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption

Apple Inc. (2016, Feb. 16). Customer Letter: Your Security and Privacy Are Important. www.apple.com/customer-letter/

AppleInsider (2025, February 21). Apple turns off data protection in the UK rather than comply with backdoor mandate. https://appleinsider.com/articles/25/02/21/apple-turns-off-data-protection-uk

Cathcart, W. (2021, Mar. 17). Why WhatsApp is pushing back on NSO Group hacking. WhatsApp Blog. https://www.business-humanrights.org/en/latest-news/commentary-why-whatsapp-is-pushing-back-on-nso-group-hacking/

CDT (2017). Center for Democracy & Technology. CDT's Comments on Law Enforcement Access to Data Stored Across Borders. https://commission.europa.eu/document/download/9fd2223e-a50e-45d9-a566-fc08967844da_en?filename=cdt_2017_en.pdf

DOJ (2019, Oct. 4). U.S. Department of Justice. Attorney General William P. Barr Delivers Remarks at the Lawful Access Summit (speech). www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit

EFF (2015, Dec. 31). Electronic Frontier Foundation. Encryption in the Balance: 2015 in Review. www.eff.org/deeplinks/2015/12/encryption-balance-2015-review

EFF (2019, Nov. 1). Electronic Frontier Foundation. Why adding client-side scanning breaks end-to-end encryption. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2022/08/why-adding-client-side-scanning-breaks-end-end-encryption

FBI (2020, Jan. 27). Federal Bureau of Investigation. Going Dark: Lawful Electronic Surveillance in the Face of New Technologies (testimony). www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

Green, M., & Smith, M. (2016). Keys under doormats, revisited. *Information Security Journal: A Global Perspective, 25*(3), 109–114.

Hartel, P., & van Wegberg, R. (2023). Going dark? Analyzing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. Crime Science, 12(5). https://doi.org/10.1186/s40163-023-00185-4

Herath, C., & Dawda, S. (2022). Balancing end-to-end encryption and public safety. Royal United Services Institute. https://static.rusi.org/325-OP-E2EE.pdf

Landau, S. (2021). Listening in: Cybersecurity in an insecure age. Yale University Press.

Law Enforcement Coalition (2018). Joint Law Enforcement Statement on Encryption and Public Safety. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Mohapatra, R. (2020). Exploring the authoritarian dimension of encryption backdoors. *Human Rights & Technology Review, 8*(1), 67–89.

Nye, J. (2011). The future of power. PublicAffairs.

Proton (2025, Feb. 25). Apple revoked Advanced Data Protection in the UK – now what? https://proton.me/blog/protect-data-apple-adp-uk

Rogers, E.M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

The Guardian (2025, Feb. 21). Apple removes advanced data protection tools in face of UK government request. https://www.theguardian.com/technology/2025/feb/21/apple-removes-advanced-data-protection-tool-uk-government

The Verge (2025a, Feb. 21). Apple pulls encryption features from the UK over government spying demand. https://www.theverge.com/news/617273/apple-removes-encryption-advanced-data-protection-adp-uk-spying-backdoor

The Verge (2025b, Feb. 28). UK will neither confirm nor deny that it's killing encryption. https://www.theverge.com/policy/621848/uk-killing-encryption-e2e-apple-adp-privacy

U.S. Congress (2020). *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020*, S. 3398, 116th Congress. www.congress.gov/bill/116th-congress/senate-bill/3398