

ARTICLE

ENCRYPTION AND GLOBALIZATION 15 YEARS LATER: END-TO-END ENCRYPTION AND THE THIRD ROUND OF THE “GOING DARK” DEBATE

*Peter Swire, Kenesa Ahmad & Michael Specter**

ABSTRACT

This Article updates and expands on 2012 research articles on encryption and globalization, analyzing what the authors call “Round 3” of the Going Dark Debate: the current controversies over end-to-end encryption (E2EE). Governments around the world have proposed, and in some cases enacted, laws limiting E2EE for law enforcement and national security purposes. This Article explains the underlying technologies and market developments for a law and policy audience to assess those proposals critically.

The Article proceeds in three parts tracking three rounds of the Going Dark Debate. Round 1 covers the Crypto Wars of the 1990s, when US export controls on strong encryption ultimately fell in 1999. Round 2 covers the period from roughly 2010 to 2015, when encryption-in-transit became widespread but lawful access remained available through cloud providers, giving rise to what the authors called a “golden age of surveillance” rather than a period of

* Peter Swire is the J.Z. Liang Chair in the School of Cybersecurity and Privacy, at the Georgia Tech College of Computing, and Professor of Law and Ethics at the Georgia Tech Scheller College of Business. He is the Research Director of the Cross-Border Data Forum. Kenesa Ahmad is the Treasurer of the Cross-Border Data Forum. Michael Specter is Assistant Professor at the School of Cybersecurity and Privacy and the School of Computer Science, at the Georgia Tech College of Computing.

For comments on earlier drafts, the authors thank Steven Bellovin, DeBrae Kennedy-Mayo, Susan Landau, Cecilia Testart, and participants of the Fordham International Law Journal Symposium on Emergent Global Trends in Data Governance and the Georgia Tech Cybersecurity and Privacy Social Science Discussion Group. Remaining errors are those of the authors. Our thanks for funding this research to the Cross-Border Data Forum, Georgia Tech School of Cybersecurity and Privacy, and Microsoft.

going dark. Round 3 addresses the current debate over E2EE, where no entity between sender and recipient can read the plaintext.

The Article's first major contribution is identifying five technically distinct scenarios for how E2EE operates in practice, each with different implications for lawful access. These scenarios reveal a substantial gap between the assumption that E2EE categorically blocks lawful access and the reality of how communications are actually sent and received. Second, the Article further shows that E2EE is not limited to messaging; instead, it is embedded throughout the modern technology stack, including in Transport Layer Security, Secure Shell, Virtual Private Networks, digital signatures, and Zero Trust Architecture, the last of which is now legally required under US and EU law. Any law broadly limiting E2EE would thus have severe consequences for cybersecurity, commerce, and government operations. The Article concludes that the two key lessons from Round 2, the least trusted country problem and the golden age of surveillance, remain true in Round 3, and that new government claims for restricting effective encryption deserve great skepticism.

I. INTRODUCTION.....	1252
II. ROUND 1: THE CRYPTO WARS OF THE 1990S	1255
A. The Technical Diagram: Blocking Wiretaps	1256
B. Round 1 of the Going Dark Debate	1257
III. ROUND 2: GLOBALIZATION AND THE 2012	
ANALYSIS	1261
A. The Technical Diagram: Access to Stored Records in the Cloud	1262
B. From Real-Time Intercepts to Records Stored in the Cloud	1263
1. The shift toward cloud computing and default encryption-in-transit.	1263
2. Implications of the shift toward cloud computing and default encryption-in-transit.	1267
C. Globalization and Encryption	1269

1. Round 2 Going Dark Concerns in the United States and Globally.....	1269
2. The “Least Trusted Country” Problem	1270
3. “Going Dark” vs. a “Golden Age of Surveillance” 1271	
IV.ROUND 3: END-TO-END ENCRYPTION	1272
A. Round 3 of the Going Dark Debates – Critiquing E2EE.....	1272
1. Significant But Far-From-Universal Rise in E2EE for Messaging	1273
2. From Jawboning to Proposed Legal Limits on E2EE	1277
B. The Technical Diagrams: Five Variations for End-to- End Encryption in Messaging	1282
1. Scenario 1: “True” or “implicitly assumed” E2EE.	1283
2. Scenario 2: The Government Can Access Content that the Device Uploads to the Cloud.	1284
3. Scenario 3: The Government Can Access Content through Software as a Service.	1285
4. Scenario 4: Software on the Device Can Give Access to the Government.	1287
5. Scenario 5: “Ghost” and Group Chats.....	1289
C. E2EE Protects Confidentiality for Far More Than Messaging.	1290
1. Transport Layer Security.	1291
2. Secure Shell.	1293
3. Virtual Private Networks.	1293
D. E2EE Beyond Confidentiality: Integrity, Authentication, and Authenticity	1294
1. Data integrity, blockchain, and digital signatures.....	1295
2. Zero-Trust Architecture and Authentication in Encryption	1296
V.CONCLUSION: POLICY LESSONS FOR ROUND 3 OF THE GOING DARK DEBATE	1298
A. Surprisingly Often, Lawful Access Can Gain Access to Messages.....	1299

B. E2EE Is Used for Multiple, Vital Layers of the Technology Stack.....	1301
C. Unintended Cybersecurity and Other Consequences of Legal Limits on E2EE.....	1303
D. Overall Conclusion: The Continued Persuasiveness of “Least Trusted Country” and “Golden Age of Surveillance”.....	1304

I. INTRODUCTION

The 2020s have seen a revival in the long-running debate about whether and how governments will impose limits on effective encryption. Governments around the globe seek to gain “lawful access” to information, notably to assist law enforcement and national security investigations. Depending on how the technology is deployed, encryption may block these sorts of investigations from gaining such access. In response, governments since the rise of the commercial Internet have proposed, and sometimes implemented, laws that restrict the use of encryption.

This Article updates and expands the 2012 article “Encryption and Globalization,”¹ by co-authors Swire and Ahmad, and the companion 2012 article by Swire on “From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud.”² As with the two previous articles, this Article explains the underlying technologies and market developments for a law and policy audience. A clear understanding of these technological and market realities, in turn, equips law and policy readers to assess new proposals to limit and otherwise govern the use of strong encryption. Notably, this sort of understanding is vital for assessing government claims that encryption limits are needed to provide lawful access for law enforcement and national security investigations.³

1. Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 437–39 (2012).

2. Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, 2 INT’L DATA PRIV. L. 200 (2012), reprinted in BULK COLLECTION: SYSTEMIC GOVERNMENT ACCESS TO PRIVATE SECTOR DATA 409, 420 (Fred H. Cate & James X. Dempsey eds., 2017).

3. For a collection of legal and related literature through 2019, see Alan Rozenshtein, *Wicked Crypto*, 9 UC IRVINE L. REV. 1181, 1182 n.4 (2019).

Part II of the Article summarizes key lessons from the “Crypto Wars” of the 1990s, when law and policy leaders became more involved in cryptography debates that until then had been held primarily in the technical community.⁴ As the commercial Internet began to develop in the 1990s, the export of strong encryption from the United States was illegal, with the stated goal of maintaining lawful access for law enforcement and national security investigations. In this first round of encryption controversy that engaged many law and policy leaders, three related arguments supported the use of strong encryption: a privacy argument to maintain the confidentiality of communications; a cybersecurity argument stressing that effective encryption was necessary to protect important activity on the Internet; and a commercial argument that strong encryption was necessary for US-based companies to sell encryption products and compete effectively online. This round of the argument, focused on US policy, effectively ended in 1999 when the US government shifted position and approved the global export of almost all encryption.

Part III of the Article explains the legal and policy debates that emerged as encryption became globally controversial by the time of the 2012 articles. By then, government agencies were facing newly prevalent use of encryption-in-transit for email, web, and many other communications. To describe the concern of government agencies, FBI lawyer Valerie Caproni introduced the term “going dark” in 2011 testimony, and the phrase became the defining image for law enforcement’s belief that it was losing visibility into encrypted content.

The 2012 articles examined how technical and market realities had changed. Lawful access continued to be possible from cloud providers. As encryption-in-transit was becoming more prevalent, making wiretaps less effective, emails and other vital

4. See Susan Landau, *Primes, Codes and the National Security Agency*, 30 NOTICES AM. MATHEMATICAL SOC’Y 7, 8–10 (1983); see also Susan Landau, *The Development of a Crypto Policy Community: Diffie-Hellman’s Impact on Public Policy*, in DEMOCRATIZING CRYPTOGRAPHY: THE WORK OF WHITFIELD DIFFIE AND MARTIN HELLMAN 231, 256 (Rebecca Slayton ed., 2022).

content were still generally technically available in unencrypted form—in “plaintext.”⁵

Given these updated technical and market realities, our 2012 article offered two key lessons for encryption in an Internet that had become heavily globalized. First, encryption policy should be developed in consideration of the “least trusted country”; that is, a proposed limit on encryption should be normatively evaluated on how one would like that power to be exercised in the country one trusts the least. This perspective was vital, because encryption broken for the benefit of one country would also be broken for the benefit of other countries, including those one trusts the least. Second, we argued that government agencies were not “going dark” when it came to their surveillance powers; instead, we had entered what we called a “golden age of surveillance.” Law enforcement and other government agencies had unprecedented and sweeping capabilities to gather information about individuals. The normative claims by governments of the need to limit encryption were thus far weaker than often believed.

Part IV of this Article analyzes what we call “Round 3 of the Going Dark Debates.” The most important technical and market change since 2012 comes from multiple uses for “end-to-end encryption” (E2EE). We define E2EE as having no one between the sender (Alice) and recipient (Bob) who can read the plaintext (the content of the communication).⁶

5. “Unencrypted form’ refers to data that is not encoded or scrambled . . . [and] allows for the inspection of traffic that is typically encrypted, such as VPN traffic or SSL connections.” *Computer Science: Unencrypted Form*, SCIENCE DIRECT, <https://www.sciencedirect.com/topics/computer-science/unencrypted-form> [https://perma.cc/B76H-WEMN] (last visited Mar. 5, 2026); see *What Is a VPN (Virtual Private Network)?*, MICROSOFT AZURE, <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn> [https://perma.cc/Q58R-GUS4] (last visited Mar. 4, 2026) (“A VPN is a foundational networking and security technology in a cloud-first world where applications span on-premises infrastructure and public cloud services.”); *What Is SSL, TLS & HTTPS?*, DIGICERT, <https://www.digicert.com/what-is-ssl-tls-and-https> [https://perma.cc/5TRC-UE6S] (last visited Mar. 4, 2026) (“SSL is standard technology for securing an internet connection by encrypting data sent between a website and a browser (or between two servers).”). Plaintext is defined as “[u]nencrypted information that may be input to an encryption operation.” *Plaintext*, NIST COMPUT. SEC. RES. CTR., <https://csrc.nist.gov/glossary/term/plaintext> [https://perma.cc/ZVP3-THKA] (last visited Mar. 4, 2026).

6. Part IV discusses five scenarios for E2EE, including the scenario we call “true” or “implicitly assumed” E2EE. In that scenario E2EE operates as defined in the text: no one between Alice and Bob can read the content, and there is no mechanism for anyone other

Under the architecture prevalent in 2012, the cloud companies positioned between Alice and Bob had access to the plaintext, allowing governments to use lawful access to seek evidence held by those providers. By contrast, with E2EE, there is no entity between Alice and Bob who can read the content of the communications. Even the cloud companies have access only to encrypted communications, so lawful access would no longer work when sought from the cloud providers.

Governments around the globe in recent years have proposed limits on E2EE. Supporters of these proposals highlight what they consider the unprecedented lack of lawful access to communications protected by E2EE. Our analysis offers reasons for great caution about claims of unprecedented and decisive loss of access for law enforcement and national security investigations. As one contribution of this Article, we explain at least five distinct scenarios that all constitute E2EE, with very different legal and policy implications. We also emphasize a point we have not seen elsewhere, that E2EE is used for many of the most important and widespread protocols used on the modern Internet. Therefore, any law or policy proposal that limits E2EE risks pervasively undermining the cybersecurity of modern computing.

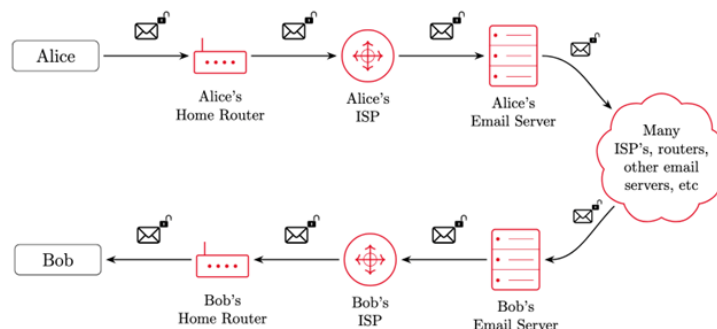
In the conclusion, in Part V, we underscore the continued importance of the two lessons from Round 2 of the Going Dark Debates—the risk posed by the least trusted country, and the continuing ways that we live in a Golden Age of Surveillance. Encryption is far more widely used than in 2012, for compelling reasons. Great skepticism should continue to apply to the claims of law enforcement and national security agencies that the law should restrict use of effective encryption.

II. ROUND 1: THE CRYPTO WARS OF THE 1990S

Part II explains how the technical architecture of the early Internet was insecure, leading to strong arguments for users being able to encrypt their communications through the Internet. Although US law enforcement and national security agencies

than Bob to read the content once it arrives. The other four scenarios all involve E2EE in the sense that no one between Alice and Bob can read the content in transit, but in each, lawful access may be possible because the content of the communication may become available to someone other than Bob.

argued vigorously for placing limits on use of strong encryption, the “Crypto Wars” of the 1990s ended with broad legal authorization for such encryption.



A. *The Technical Diagram: Blocking Wiretaps*

Diagram 1: Insecurity of Unencrypted Communications on the Internet

Diagram 1 illustrates the rationale for effective encryption in the 1990s, as the commercial internet began to develop. In the illustration, Alice wishes to send an email to Bob. The security and privacy problem is that an unencrypted message can be intercepted and read at multiple steps before the message reaches Bob. Consider a few examples of how this interception can occur: (1) the Internet Service Provider for Alice or Bob can monitor the content of all of their traffic;⁷ (2) malicious hackers can read the plaintext as the message goes across the Internet; (3) law enforcement and national security agencies can “wiretap,” intercepting the plaintext as the message goes from Alice to Bob.

7. Alissa Cooper, *The Privacy Risks of ISPs Using Deep Packet Inspection*, CTR. FOR DEMOCRACY & TECH. (July 1, 2010), <https://cdt.org/insights/the-privacy-risks-of-isps-using-deep-packet-inspection/> [<https://perma.cc/TD9K-2V3F>]; see *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies: Hearing Before the Subcomm. on Telecomms. & the Internet of the H. Comm. on Energy & Com.*, 110th Cong. (2008) (statement of Alissa Cooper, Chief Comput. Scientist, Ctr. for Democracy & Tech.).

B. Round 1 of the Going Dark Debate

Round 1 of the Going Dark debate began in the early 1990s, as private-sector use of encryption started to become a significant potential barrier to lawful access. Before 1990, cryptography was dominated by government agencies. Strong encryption was a tool of intelligence services and the military,⁸ not of commercial software or ordinary users. That began to change in the 1990s, when the RSA algorithm spread into commercial use.⁹ RSA's public-key encryption¹⁰ gave businesses and ordinary users access to strong encryption for the first time.

8. The famous breaking of the German Enigma code was an example of military efforts to break encryption used by the German government. See DAVID KAHN, *SEIZING THE ENIGMA: THE RACE TO BREAK THE GERMAN U-BOAT CODES, 1939–1943* (1991); Susan Borowski, *Code-Breaking Instrumental in Ending World War II*, AM. ASS'N FOR ADVANCEMENT SCI. (Dec. 12, 2012), <https://www.aaas.org/membership/scientia/code-breaking-instrumental-ending-world-war-ii> [<https://perma.cc/RRC5-Z8MX>]; see also David A. Hatch, *ENIGMA and PURPLE: How the Allies Broke German and Japanese Codes During the War*, in CODING THEORY AND CRYPTOGRAPHY 53, 53–61 (David Joyner ed., 2000).

9. The development of RSA encryption began in the 1970s and its usage remains influential through current day. In 1977, Scientific American (a science magazine) published a short article entitled “Mathematical Games,” authored by Martin Gardner, which provided an overview of the concept of public key encryption. See Steve Ellis, *The Day Cryptography Changed Forever*, MEDIUM (Jan. 6, 2020), <https://medium.com/swlh/the-day-cryptography-changed-forever-1b6aefe8bda7> [<https://perma.cc/KP76-PAZK>]. In 1978, Ronald Rivest, Adi Shamir, and Leonard Adleman—three researchers at the Massachusetts Institute of Technology (MIT)—“discovered an elegant algorithm based on the product of two prime numbers” referred to as RSA encryption, an acronym representing the initials of these inventors. Gerritt Bleumer, *Nonsecret Encryption*, in ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY 424, 425 (Henk C.A. Tilborg ed., 2005). In the United States, the patent for RSA encryption was issued to MIT in 1983. See Simson Garfinkel, *5 MIT Patents That Changed Computing*, MIT TECH. REV. (Feb. 23, 2022), <https://www.technologyreview.com/2022/02/23/1044184/5-mit-patents-that-changed-computing/> [<https://perma.cc/5EHF-3VC6>]; Ann Harrison, *RSA Encryption Patent Released*, COMPUTERWORLD (Sept. 18, 2020), <https://www.computerworld.com/article/1358428/rsa-encryption-patent-released.html> [<https://perma.cc/K7S7-N4LF>]. As of this writing, RSA is one of “the world’s most widely used public-key cryptography method[s] for securing . . . the internet” for usages such as email, virtual private networks (VPNs), and e-commerce. *RSA Cryptography: The Algorithm Keeping Us Safe Online*, NAT’L INVS. HALL FAME (Nov. 13, 2019), <https://www.invent.org/blog/inventors/rsa-cryptography-algorithm> [<https://perma.cc/VG6S-XUR9>]; see *RSA Security: From Public Key Cryptography Breakthroughs to the Future of Identity Security*, RSA, <https://www.rsa.com/company/rsa-cryptography/> [<https://perma.cc/YB9G-FXYZ>] (last visited Mar. 10, 2026).

10. See Tom Krantz & Alexandra Jonker, *What Is Public Key Encryption?*, IBM, <https://www.ibm.com/think/topics/public-key-encryption> [<https://perma.cc/TH89-MLLK>] (last visited Mar. 14, 2026).

In the United States, encryption was treated as a “munition,” with legal limits on exporting strong encryption to other countries.¹¹ Strong encryption was permitted for use within the United States, but exports had to deploy intentionally weakened encryption.¹² This logic is similar to the regulation of other “dual-use” technologies, which can be used for both civilian and military purposes.¹³ As with advanced technology for fighter jets, the idea was that advanced encryption technology could help adversaries and hurt the United States and its allies. From a military point of view, that concern makes sense—recall that during World War II the Allies gained a secret and decisive intelligence edge by breaking the German Enigma code.¹⁴ With this history in mind, one can understand why national security agencies wanted to limit the risk that advanced encryption would fall into the hands of adversary nations.

Along with these national security considerations, the Federal Bureau of Investigation (FBI) and other law enforcement agencies had their own reason to worry about the spread of strong encryption. If the message is encrypted in transit between Alice and Bob, the FBI’s wiretap will fail—it will only capture encrypted messages, which the FBI is not able to read. To understand the law enforcement perspective, consider that US law permits wiretaps only for serious crimes, and only when other methods of investigation have been tried and failed, reasonably appear unlikely to succeed, or would be too dangerous.¹⁵ Criminal prosecutors face the high standard of proving an individual guilty

11. Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th and the 21st Centuries*, in *THE HISTORY OF INFORMATION SECURITY: A COMPREHENSIVE HANDBOOK* 725, 725–36 (Karl de Leeuw & Jan Bergstra eds., 2007).

12. *Id.*; see STEVEN LEVY, *CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT SAVING PRIVACY IN THE DIGITAL AGE* (2012).

13. See Peter Swire & Samm Sacks, *Personal Data as a Dual-Use Technology: Critically Assessing the New Alliance of Privacy and National Security*, 66 VA. J. INT’L L. 419, 426–37 (2026); see also Swire & Ahmad, *supra* note 1, at 437–39.

14. See Hatch, *supra* note 8, at 53–61.

15. According to Title III, an application for a wiretap requires “a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.” 18 U.S.C. § 2518(1)(c). Title III “limited wiretaps to specific serious crimes and only as a last resort when other investigative techniques had been exhausted.” Kristopher A. Nelson, *Transnational Wiretaps and the Fourth Amendment*, 36 HASTINGS CONST. L.Q. 329, 333 (2009); see SUSAN LANDAU ET AL., ASS’N FOR COMPUTING MACH. INC., *CODES, KEYS AND CONFLICTS: ISSUES IN U.S. CRYPTO POLICY* (1994) [hereinafter *ACM REPORT*].

“beyond a reasonable doubt.”¹⁶ For an ongoing and important investigation, such as one targeting organized crime, the words in a telephone call or email may be crucial to proving the individual guilty.¹⁷ Even if the prosecutor can show that Defendant 1 called Defendant 2, that may be insufficient to convict Defendant 2 unless statements from the conversation show that Defendant 2 was part of the conspiracy.¹⁸

Formidable opposition developed against these national security and law enforcement perspectives, organized around three arguments that would recur throughout the encryption debates. Privacy advocates argued that encryption was essential to limiting government surveillance.¹⁹ Security experts explained that weakening encryption would drastically reduce the security of data on the network.²⁰ The technology industry argued that business on the Internet required strong encryption and that Silicon Valley and US e-commerce depended on global acceptance of American commercial technology.²¹ One fundamental argument was that important activities would not grow on the Internet if anyone between Alice and Bob could easily intercept their communications.²²

This soon collided with the government’s “Clipper Chip” proposal, the first major encryption policy battle of the 1990s

16. *Amdt14.S1.5.5.5 Guilt Beyond a Reasonable Doubt*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt14-S1-5-5-5/ALDE_00013763/ [<https://perma.cc/22G3-ABT2>] (last visited Mar. 10, 2026).

17. New America, *Debate on Law Enforcement vs. Smartphone Encryption: Is FBI “Going Dark” or in a Golden Age of Surveillance?*, YOUTUBE (Nov. 17, 2014), <https://www.youtube.com/watch?v=6NVmsn6yuS4> [<https://perma.cc/3MT4-7QDG>].

18. Although the government emphasized accessing the content of communications, metadata about the communication (to/from, date, length, etc.) generally remains available. Former National Security Agency Director Michael Hayden said, for instance, that “we kill people based on metadata.” David Cole, *“We Kill People Based on Metadata”*, N.Y. REV. BOOKS (May 10, 2014), <https://www.nybooks.com/online/2014/05/10/we-kill-people-based-metadata/> [<https://perma.cc/W5FM-STR8>].

19. Kevin Bankston, Andi Wilson Thompson & Danielle Kehl, *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s*, NEW AM. (June 2015), <https://www.newamerica.org/insights/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/> [<https://perma.cc/5X5P-CXQU>] [hereinafter *Doomed to Repeat History?*]; KRISTIN FINKLEA, CONG. RSCH. SERV., IF11769, LAW ENFORCEMENT AND TECHNOLOGY: THE “LAWFUL ACCESS” DEBATE (updated Jan. 12, 2026) [hereinafter *LAWFUL ACCESS DEBATE*].

20. See Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, 2 WORLD WIDE WEB J. 241, 248 (1997) [hereinafter *Risks of Key Recovery*].

21. See *Doomed to Repeat History?*, *supra* note 19, at 13.

22. See *id.* at 13–14.

concerning the US government.²³ Although the details evolved over time, the Bush and then Clinton administrations supported having some way to gain access via hardware chips.²⁴ This was a “key escrow” proposal: the government would hold copies of stored (“escrowed”) encryption keys, which could be accessed with judicial approval. The government’s position held that because judicial approval worked for a telephone wiretap, it should also work for Internet communications.²⁵

The Clipper Chip and related government proposals encountered ferocious opposition. Computer scientist Matt Blaze showed a technical flaw in the Clipper Chip design,²⁶ and a distinguished set of technical experts wrote an influential explanation of the risks arising from key escrow.²⁷ With apologies to all Crypto War veterans not cited: prominent encryption and computer scientists issued statements, and studies organized by groups such as the Computer Professionals for Social Responsibility and the Center for Democracy and Technology (CDT).²⁸ CDT organized a report from a group of thirty law professors, with co-author Swire as a drafter, along with Michael Froomkin²⁹ and Lawrence Lessig.³⁰ Industry groups also strongly opposed the government position on encryption.³¹

23. For an overview of the history of the key-escrow policy, see Craig Jarvis & Keith M. Martin, *A Milestone in Encryption Control – What Sank the US Key-Escrow Policy?*, 39 INTEL. & NAT’L SEC. 986 (2024).

24. See Swire & Ahmad, *supra* note 1, at 437–39.

25. A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 797 (1995).

26. John Markoff, *At AT&T, No Joy on Clipper Flaw*, N.Y. TIMES (June 3, 1994), <https://www.nytimes.com/1994/06/03/business/at-at-t-no-joy-on-clipper-flaw.html> [<https://perma.cc/XX84-V45H>]; see Matt Blaze, *Key Escrow from a Safe Distance: Looking Back at the Clipper Chip*, ACSAC, <https://www.acsac.org/2011/program/keynotes/blaze.pdf> [<https://perma.cc/F58A-FFCL>] (last visited Mar. 14, 2026).

27. *Risks of Key Recovery*, *supra* note 20, at 241.

28. Letter from Crypto Experts to William J. Clinton, President of the U.S. (Jan. 27, 1994), https://archive.epic.org/crypto/clipper/crypto_experts_letter_1_94.html [<https://perma.cc/HAH4-NCQR>]; *Risks of Key Recovery*, *supra* note 20, at 241.

29. For a detailed legal analysis of Clipper Chip proposals, see Froomkin, *supra* note 25.

30. Letter from Law Professors to the H. Comm. on Com., *Opposing Mandatory Key Escrow* (Sept. 23, 1997), <https://osaka.law.miami.edu/froomkin/lawprof-letter.htm> [<https://perma.cc/W8VD-BTRK>].

31. Jarvis & Martin, *supra* note 23, at 992.

The campaign to allow strong encryption was effective.³² The Clipper Chip was abandoned by 1996,³³ although the government's support for encryption limits continued. The decisive change in administration policy was announced in September 1999.³⁴ At a briefing at which co-author Swire spoke,³⁵ the White House declared that almost all the export controls on encryption were being lifted.³⁶ The arguments for privacy, computer security, and US-based global commerce won, and the "Crypto Wars" of the 1990s came to a close.

III. ROUND 2: GLOBALIZATION AND THE 2012 ANALYSIS

Part III discusses what we call "Round 2" of the Going Dark Debates. During the period from roughly 2010 to 2015, encryption-in-transit became increasingly important, and encryption policy debates went global, as countries including India and China considered limits on encryption. Part III also explains key arguments from the 2012 writing by Swire and Ahmad, including that it was a "golden age of surveillance," rather than being a time when government agencies were "going dark."

32. Susan Landau, Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure, 7 J. NAT'L SEC. L. & POL'Y 411, 424–26 (2014).

33. Jarvis & Martin, *supra* note 23, at 992.

34. Press Briefing, The White House, Special White House Briefing: Encryption Technology (Sept. 16, 1999), https://w2.eff.org/Privacy/Crypto_export/1999_export_policy/19990916_wh_briefing_transcript.html [<https://perma.cc/5H5P-CVXH>] [hereinafter Encryption Briefing].

35. At the time, Swire was the Chief Counselor for Privacy, in the US Office of Management and Budget. See *Professor Joins Administration to Handle Privacy Issues*, N.Y. TIMES (Mar. 5, 1999), <https://archive.nytimes.com/www.nytimes.com/library/tech/99/03/biztech/articles/05privacy.html> [<https://perma.cc/SK4G-HCPJ>]. He chaired the White House Working Group on Encryption in 1999, leading up to the September announcement. See *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 36 (2015) (statement of Peter Swire, Huang Professor of Law & Ethics, Scheller Coll. of Bus., Ga. Inst. of Tech.) [hereinafter *Going Dark 2015 Hearing*]; Press Briefing, The White House, Press Briefing by Deputy National Security Advisor Jim Steinberg, Attorney General Janet Reno, Deputy Secretary of Defense John Hamre, Under Secretary of Commerce Bill Reinsch, and Chief Counselor for Privacy at OMB Peter Swire (Sept. 16, 1999), <https://peterswire.net/archive/privarchives/Press%20briefing%20Sept.%2016%201999.html> [<https://perma.cc/A2GD-DATG>]. Swire had also written previously on encryption and the law. Peter P. Swire, *The Uses and Limits of Financial Cryptography: A Law Professor's Perspective*, in FINANCIAL CRYPTOGRAPHY: FIRST INTERNATIONAL CONFERENCE, FC '97 239 (Rafael Hirschfeld ed., 1997).

36. The announcement also promised the FBI and Department of Justice technical assistance funding to update their capabilities. Encryption Briefing, *supra* note 34.

A. The Technical Diagram: Access to Stored Records in the Cloud

Diagram 2 illustrates the commercially important configuration that was emerging by 2012. In the illustration, Alice still wishes to send an email to Bob, but two major things have changed as a technical and business matter since Round 1 of the Going Dark debate. First, a large and growing proportion of emails and other Internet traffic was now “encrypted in transit.” As a result, strong encryption blocks wiretaps from accessing the content as it travels between Alice and her email provider, between her email provider and Bob’s email provider, and between Bob’s email provider and Bob. Second, email and a growing fraction of other Internet traffic had begun to be stored in the cloud.³⁷

The combination of encryption-in-transit and cloud storage had a crucial implication for law enforcement access: emails and a great deal of other information was available in plaintext in the cloud. Therefore, a court order served on the cloud provider could retrieve the full communication between Alice and Bob.

Cloud computing became increasingly common by 2012. Diagram 2 illustrates both points: wiretaps would no longer work for communications in transit, but law enforcement access remained possible if the government could gain access to stored communications in the cloud.

37. As discussed below, cloud computing and storage was much less common during Round One, when stored information was more often only on Alice and Bob’s devices.

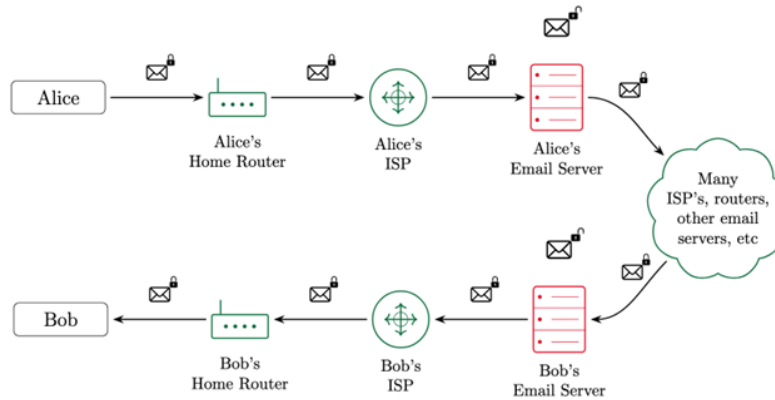


Diagram 2: Law Enforcement Can Get Access at Email Provider

B. From Real-Time Intercepts to Records Stored in the Cloud

The 2012 *Stored Communications* article documented the shift toward cloud computing and default encryption-in-transit, as shown in Diagram 2. This shift had important legal and policy implications, putting significant pressure on the international system for cooperative law enforcement investigations conducted under Mutual Legal Assistance Treaties (MLATs).

1. The shift toward cloud computing and default encryption-in-transit.

The commercial importance of encryption grew only gradually after the 1999 close of Round 1 of the Going Dark Debate. Once strong encryption was legal for global commerce, a growing number of business users, such as financial services, adopted encryption for their communications on the Internet.³⁸ The

38. See NAT'L ACADS. OF SCIS., ENG'G & MED., DECRYPTING THE ENCRYPTION DEBATE: A FRAMEWORK FOR DECISION MAKERS 16 (2018); JAMES A. LEWIS, DENISE E. ZHENG & WILLIAM A. CARTER, CTR. FOR STRATEGIC & INT'L STUD., THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA 2 (2017), <https://csis-website-prod.s3.amazonaws.com/s3fs->

communications of most ordinary users, however, typically remained unencrypted. Text messages and emails were unencrypted on most services.³⁹ Web surfing was done overwhelmingly with the HTTP protocol, and not the encrypted and more secure HTTPS.⁴⁰ As one sign of how rarely encryption was encountered, the Department of Justice (DOJ) was required by law to report the number of investigations where encryption was involved—in 2012 that figure was only fifteen out of over 3,000 wiretap investigations.⁴¹

By about 2012, cloud services emerged as a large and growing portion of commercial and individual computing. Few companies used cloud services in 1999,⁴² and Amazon Web Services did not launch until 2006;⁴³ yet by 2012, seventy-four percent of companies globally had adopted some sort of cloud services.⁴⁴ Gmail's launch in 2004 marked a crucial shift towards cloud storage and its implications for law enforcement's access to email content. At that time, leading webmail services offered by Yahoo! and Microsoft stored thirty to sixty emails; Gmail's offer of a

public/publication/170221_Lewis_EncryptionsEffect_Web.pdf [https://perma.cc/9FWU-H6P7].

39. See NAT'L ACADS. OF SCIS., ENG'G & MED., *supra* note 38, at 16; LEWIS ET AL., *supra* note 38, at 2.

40. See *Upgrade to Core HTTP Protocol Promises Speedier, Easier Web*, CONVERSATION (Feb. 19, 2015), <https://theconversation.com/upgrade-to-core-http-protocol-promises-speedier-easier-web-37690> [https://perma.cc/M9E4-ZQ6Z]; LEWIS ET AL., *supra* note 38, at 5.

41. In 2012, the DOJ reported fifteen domestic wiretaps where encryption was involved. *Wiretap Report 2012*, U.S. COURTS (Dec. 31, 2012), <https://www.uscourts.gov/data-news/reports/statistical-reports/wiretap-reports/wiretap-report-2012> [https://perma.cc/NL5L-ETPX]. During that same year, DOJ reported 3,380 wiretaps where encryption was not present. Andrea O'Sullivan & Eli Dourado, *Going Dark? Federal Wiretap Data Shows Scant Encryption Problems*, MERCATUS CTR. 2 (Feb. 26, 2016), <https://www.mercatus.org/research/data-visualizations/going-dark-federal-wiretap-data-show-scant-encryption-problems> [https://perma.cc/QT34-DVYH]. "Notably, these data do not capture instances in which law enforcement officials know they will encounter 'warrant-proof' encryption, and thus they elect not to attempt intercepting and breaking the encryption on the communication." KRISTIN FINKLEA, CONG. RSCH. SERV., R44481, ENCRYPTION AND THE "GOING DARK" DEBATE 6-7 (2016) [hereinafter GOING DARK DEBATE].

42. See Keith D. Foote, *A Brief History of Cloud Computing*, DATAVERSITY (Dec. 17, 2021), <https://www.dataversity.net/articles/brief-history-cloud-computing/> [https://perma.cc/B67L-RCEX].

43. *Id.*

44. Pete Mann, *Rise of the Cloud*, CONSULTING MAG. (July 21, 2012), <https://www.consultingmag.com/2012/07/21/rise-of-the-cloud/> [https://perma.cc/MK45-GE3T].

gigabyte of free storage increased that number to about 13,500.⁴⁵ Before Gmail launched in 2004, most emails were downloaded to the user's device and deleted from the server, so law enforcement typically needed access to the user's device to read the content.⁴⁶ After the spread of Gmail and other cloud-based email storage services, law enforcement with a search warrant could typically gain access to email content from the provider.

As documented in Swire's 2012 article, an increasing portion of consumer communications began to be encrypted in transit. For instance, Hotmail and Gmail encrypted emails to the server, and virtual private networks had become common.⁴⁷ The trend toward encryption continued after June 2013, when Edward Snowden, a contractor for the National Security Agency (NSA), disclosed a large cache of classified documents describing the scope of US government surveillance programs.⁴⁸ Concerns were substantial within the United States and magnified abroad, as US-based service providers had to answer questions from regulators and the public about whether the NSA had access to people's daily online communications.⁴⁹

45. Associated Press, *Gmail Revolutionized Email 20 Years Ago*, NBC NEWS (Mar. 31, 2024), <https://www.nbcnews.com/news/us-news/gmail-revolutionized-email-20-years-ago-rcna145777> [<https://perma.cc/N7Y4-VFCQ>] [hereinafter *Gmail Revolution*].

46. "POP3 is designed to download emails from the server to a local device, often deleting them from the server afterward, making it suitable for single-device email management." Kirsten Peremore, *What Are POP3 and IMAP?*, PAUBOX (Nov. 22, 2024), <https://www.paubox.com/blog/what-are-pop3-and-imap> [<https://perma.cc/K7WS-V6YS>]. Prior to Gmail's launch in 2004, the email landscape was dominated by the use of POP3. See *POP3 (Post Office Protocol Version 3)*, FS (June 10, 2025), <https://www.fs.com/glossary/pop3-post-office-protocol-version-3-g549.html> [<https://perma.cc/9TZF-UHUQ>]; *Gmail Revolution*, *supra* note 45.

47. See Swire, *supra* note 2, at 202–03.

48. Snowden disclosed "more than 1.5 million classified documents from secure NSA servers." H. PERMANENT SELECT COMM. ON INTEL., 114TH CONG., REVIEW OF UNAUTHORIZED DISCLOSURES OF FORMER NATIONAL SECURITY AGENCY CONTRACTOR EDWARD SNOWDEN, at i (2016); see Ewen MacAskill & Gabriel Dance, *NSA Files Decoded: What the Revelations Mean for You*, GUARDIAN (Nov. 1, 2013), <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> [<https://perma.cc/9FTS-TP95>].

49. For instance, in the 2015 *Schrems I* case, the Court of Justice of the European Union (CJEU) found that the NSA was engaged in "indiscriminate surveillance" which resulted in "mass and undifferentiated" access to personal data. Case C-362/14, *Schrems v. Data Prot. Comm'r*, ECLI:EU:C:2015:650, ¶¶ 31, 33 (Oct. 6, 2015). In sworn testimony, Swire has documented that some of the sources cited by the CJEU exaggerated the scope of the NSA surveillance, but the Court's description illustrates the widespread concern about broad NSA surveillance. Peter Swire, *Testimony in Irish High Court Case*, Chapter 3:

The Snowden disclosures drove an important shift toward default encryption. Web traffic before 2013 was often unencrypted. Beginning in 2014, major technology companies and standards organizations launched a coordinated effort to make HTTPS, the web's encrypted protocol, the default for all web traffic—a shift discussed further in Part IV.⁵⁰ More broadly, “encryption in transit” and “encryption at rest” became more widely used for stored data.⁵¹ The default similarly shifted for device encryption. In September 2014, Apple announced that iOS 8, the latest version of its proprietary mobile operating system, would encrypt the contents of iPhones by default, using a key derived from the user's passcode, a key that Apple itself would not hold.⁵² Google announced similar plans for its Android.⁵³ These decisions meant that the companies could not unlock a device on law enforcement's behalf even with a valid warrant, because they did not possess the means to do so.⁵⁴

Systemic Safeguards in the US System of Foreign Intelligence Law, at 3-21 to 3-22 (Nov. 2, 2016), <https://www.alston.com/-/media/files/insights/publications/peter-swire-testimony-documents/chapter-3—systemic-safeguards-in-the-us-sytem-of.pdf> [https://perma.cc/GCA4-52DJ].

50. *About Let's Encrypt*, LET'S ENCRYPT, <https://letsencrypt.org/about/> [https://perma.cc/9DD4-LXSK] (last visited Mar. 10, 2026); see Peter Eckersley, *Launching in 2015: A Certificate Authority to Encrypt the Entire Web*, ELEC. FRONTIER FOUND. (Nov. 18, 2014), <https://www.eff.org/deeplinks/2014/11/certificate-authority-encrypt-entire-web> [https://perma.cc/37HQ-Z8MH]; see also Klint Finley, *Encrypted Web Traffic More Than Doubles After NSA Spying Reports*, WIRED (May 16, 2014), <https://www.wired.com/2014/05/sandvine-report/> [https://perma.cc/H39M-JJX5].

51. Andi Wilson Thompson & Claire Park, *Privacy's Best Friend: The Importance of Encryption in Protecting Consumer Privacy*, NEW AM. 7-9 (Aug. 2020), <https://www.newamerica.org/insights/privacys-best-friend/> [https://perma.cc/4U9X-9GTQ]; see Finley, *supra* note 50; Christopher Soghoian, *Snowden's Leaks Have Finally Forced Companies to Enhance Their Security*, MIT TECH. REV. (Dec. 17, 2013), <https://www.technologyreview.com/2013/12/17/14482/snowdens-leaks-have-finally-forced-companies-to-enhance-their-security/> [https://perma.cc/WC6B-YK8E].

52. Yixuan Long, *Apple Provides Default Encryption that Protects Data Stored on Device*, HARV. J.L. & TECH.: DIG. (Oct. 16, 2014), <https://jolt.law.harvard.edu/digest/apple-provides-default-encryption-that-protects-data-stored-on-device> [https://perma.cc/79ZV-TZKT].

53. Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC NEWS (Sept. 19, 2014), <https://www.bbc.com/news/technology-29276955> [https://perma.cc/9K6Y-B755].

54. As another example, the NSA and its British counterpart, GCHQ, had tapped the private fiber-optic links connecting Google's data centers. Those links carried data without encryption at the time because they were internal company infrastructure, not public-facing connections. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide*, WASH. POST (Oct. 30, 2013), <https://www.washingtonpost.com/>

2. Implications of the shift toward cloud computing and default encryption-in-transit.

These shifts toward cloud computing and default encryption-in-transit had important legal and policy implications. For US law enforcement and intelligence agencies, seeking stored records from US providers worked reasonably well: law enforcement agencies could use court orders under the Electronic Communications Privacy Act (ECPA).⁵⁵ National security investigations similarly could use legal processes under the Foreign Intelligence Surveillance Act.⁵⁶

Non-US governments faced a harder path. The ECPA provides that a non-US government can gain access to the content of emails and other communications only with a court order issued by a US judge.⁵⁷ For non-US governments, the lack of direct access to content held by US service providers placed new pressure on the Mutual Legal Assistance Treaties (MLATs) system, the cumbersome process by which a foreign government can have a US judge issue a court order on a US service provider.⁵⁸ Determining how to address this challenge became the focus of Swire's research program under the Georgia Tech Cross-Border Access to Data

world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html [https://perma.cc/V6NH-PKML]. Google subsequently encrypted the links between its data centers, followed by other companies. Jennifer Garnett, *Google Encrypts Its Network to Counteract NSA Surveillance*, HARV. J.L. & TECH.: DIG. (Nov. 18, 2013), https://jolt.law.harvard.edu/digest/google-encrypts-its-network-to-counteract-nsa-surveillance [https://perma.cc/NQW2-SF39]; Zack Whittaker, *Microsoft to Encrypt Network Traffic Amid NSA Datacenter Link Tapping Claims*, ZDNET: BUS. (Nov. 27, 2013), https://www.zdnet.com/article/microsoft-to-encrypt-network-traffic-amid-nsa-datacenter-link-tapping-claims/ [https://perma.cc/562C-92P4].

55. Wiretap Act, 18 U.S.C. §§ 2510–2522; Stored Communications Act, 18 U.S.C. §§ 2701–2712; see Reema Shah, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 YALE L.J. 543 (2015).

56. 50 U.S.C. §§ 1801–1885c; see Joris V.J. van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 ME. L. REV. 487 (2014).

57. Jennifer Daskal & Andrew K. Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, LAWFARE (Aug. 1, 2016), https://www.lawfaremedia.org/article/congress-should-embrace-doj-s-cross-border-data-fix-0 [https://perma.cc/2U5N-NE3A].

58. For discussion, see Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687 (2017); Peter Swire et al., *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 102 (2017).

Project,⁵⁹ followed by the establishment of a think tank, the Cross-Border Data Forum (CBDF), in 2018.⁶⁰

Significant MLAT reform came with the 2018 enactment of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which made two distinct changes.⁶¹ First, the CLOUD Act clarified that the US government court orders for emails and other communications extend to data even when it is stored outside of the United States—resolving the question then before the Supreme Court in the Microsoft Ireland litigation.⁶² Second, the CLOUD Act created a framework for bilateral agreements, allowing qualifying foreign governments to request data directly from US providers without going through a US judge.⁶³

The CLOUD Act has not, however, provided a mechanism for most non-US governments to gain access to emails and other content stored in the cloud. The United States has only finalized bilateral CLOUD Act agreements with the United Kingdom and Australia.⁶⁴ In the absence of such an agreement, non-US governments have an incentive to require the storage of emails and

59. *Georgia Tech Cross-Border Access to Data Project*, PETER SWIRE: RSCH. PROJECTS, <https://peterswire.net/cross-border-requests-data-project/> [<https://perma.cc/T5Y4-9EMY>] (last visited Mar. 10, 2026).

60. *Mission*, CROSS-BORDER DATA F., <https://www.crossborderdataforum.org/mission/> [<https://perma.cc/CJ5N-UUU9>] (last visited Mar. 10, 2026).

61. Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 348, 1213–25 (2018) (codified as amended in scattered sections of 18 U.S.C.). For explanation of the CLOUD Act, see Peter Swire & Jennifer Daskal, *Frequently Asked Questions About the U.S. CLOUD Act*, CROSS-BORDER DATA F. (Apr. 16, 2019), <https://www.crossborderdataforum.org/cloudactfaqs/> [<https://perma.cc/Z45Q-B8UQ>] [hereinafter *CLOUD Act FAQ*].

62. 18 U.S.C. § 2713; see Jennifer Daskal & Peter Swire, *Why the CLOUD Act Is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018), <https://www.lawfaremedia.org/article/why-cloud-act-good-privacy-and-human-rights> [<https://perma.cc/UF29-DYWQ>].

63. 18 U.S.C. § 2523(b); see CONG. RSCH. SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT (2018) (citing numerous articles co-authored by Peter Swire).

64. See Paul Greaves & Peter Swire, *New Developments for the U.K. and Australian Executive Agreements with the U.S. under the CLOUD Act*, CROSS-BORDER DATA F. (July 19, 2020), <https://www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/> [<https://perma.cc/UF47-AJL5>]; see also Peter Swire, *Comments on the Australian Legislation to Enable the Negotiation of a U.S. CLOUD Act Executive Agreement*, CROSS-BORDER DATA F. (May 11, 2020), <https://www.crossborderdataforum.org/comments-on-australian-legislation-to-enable-the-negotiation-of-a-u-s-cloud-act-executive-agreement/> [<https://perma.cc/8X85-AZB7>].

other content within their countries, in order to apply their own legal processes to gain access to that evidence.⁶⁵

C. Globalization and Encryption

The shift toward cloud computing and default encryption-in-transit shown in Diagram 2 had important implications for encryption policy in increasingly globalized communications. Although wiretaps became less effective over time, due to blocking by encryption-in-transit, our writings during Round 2 identified two insights that remain central to the rationale for enabling strong encryption: the “least trusted country” problem and the fact that we are not “going dark” but, instead, are in a “golden age of surveillance.”⁶⁶

1. Round 2 Going Dark Concerns in the United States and Globally

Law enforcement and national security wiretaps grew increasingly ineffective as encryption-in-transit became the default for email and web traffic.⁶⁷ In the United States, law enforcement and intelligence agencies once again raised alarms about losing access to communications. The term “going dark” became the tag-phrase for the encryption issue, after FBI General

65. Such data localization requirements can create conflicts of law, where the ECPA prohibits disclosure to the non-US government, but local law may require disclosure. See Theodore Christakis, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities after the CLOUD Act: Is There a Conflict with the GDPR?*, CROSS-BORDER DATA F. (June 13, 2019), <https://www.crossborderdataforum.org/transfer-of-eu-personal-data-to-u-s-law-enforcement-authorities-after-the-cloud-act-is-there-a-conflict-with-the-gdpr/> [https://perma.cc/A89S-6V4K]; *CLOUD Act FAQ*, supra note 61; see also Kenneth Propp, *Lawfare – Navigating Toward an EU-U.S. Agreement on Electronic Evidence*, CROSS-BORDER DATA F. (Dec. 7, 2023), <https://www.crossborderdataforum.org/lawfare-navigating-toward-an-eu-u-s-agreement-on-electronic-evidence/> [https://perma.cc/26LA-QHNV].

66. Peter Swire & Kenesa Ahmad, “Going Dark” Versus a “Golden Age for Surveillance”, CTR. FOR DEMOCRACY & TECH. (Nov. 28, 2011), <https://cdt.org/insights/going-dark-versus-a-golden-age-for-surveillance> [https://perma.cc/Q43K-WYR8].

67. As discussed below, some text messages were end-to-end encrypted beginning in 2011, but other leading text services, such as Facebook Messenger and Instagram, remained available at the server in plaintext. See Lily Hay Newman, *Why It Took Meta 7 Years to Turn on End-to-End Encryption for All Chats*, WIRED (Dec. 7, 2023), <https://www.wired.com/story/meta-messenger-instagram-end-to-end-encryption/> [https://perma.cc/P67Z-LUEQ].

Counsel Valerie Caproni used it in her congressional testimony in February 2011.⁶⁸

Other countries faced even greater obstacles to law enforcement and national security investigations because of the ECPA limits on providing content to non-US governments. India threatened to ban BlackBerry services unless its manufacturer, Research In Motion (RIM), gave law enforcement access to encrypted messages, a demand that intensified after the 2008 Mumbai attacks.⁶⁹ RIM eventually complied, providing plaintext of consumer messages to Indian authorities.⁷⁰ China took a different approach, proposing to block widely used international encryption standards in favor of weaker, government-accessible alternatives. As with jawboning, China used market access to pressure compliance, requiring foreign firms to adopt its domestic WAPI standard. US and international pressure eventually forced China to abandon the mandate.⁷¹

2. The “Least Trusted Country” Problem

Our 2012 article’s first major conclusion was what we called the “least trusted country” problem:

The U.S. encryption debates during the 1990s focused primarily on the best policy for one nation, the United States. A repeated criticism of the Clipper Chip was the lack of trust that the United States would escrow the encryption keys securely, or use its decryption powers wisely. In a globalized setting, the consequences of limiting encryption are much

68. We call this capabilities gap the ‘Going Dark’ problem. As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage – evidence that a court has authorized the government to collect.

Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary, 112th Cong. 6 (2011) (statement of Valerie Caproni, General Counsel, FBI) [hereinafter *Going Dark 2011 Hearing*].

69. *Blackberry Makes Offer to India Ahead of Ban Deadline*, BBC NEWS (Aug. 26, 2010), <https://www.bbc.com/news/technology-11102314> [<https://perma.cc/YFA9-6BNU>].

70. Ananya Mohanty, *The Encryption Debate in India*, CARNEGIE ENDOWMENT FOR INT’L PEACE (May 2019), <https://carnegieendowment.org/posts/2019/05/the-encryption-debate-in-india?lang=en> [<https://perma.cc/Q8UW-7RA5>].

71. Lorand Laskai & Adam Segal, *The Encryption Debate in China*, CARNEGIE ENDOWMENT FOR INT’L PEACE (May 30, 2019), <https://carnegieendowment.org/posts/2019/05/the-encryption-debate-in-china?lang=en> [<https://perma.cc/UG4B-RX4N>].

more dire if key escrow or other limits are imposed in a dozen, 50, or 200 countries. How much trust would India place in its communications in the hands of Pakistan, China in the hands of Taiwan, and so forth? As the debate shifts from a setting of one to many nations, the level of trust placed in data traveling through the Internet becomes that of the country that we trust least.⁷²

Though published in 2012, this conclusion continues to apply today. Users around the world increasingly rely on the same devices, software, and services.⁷³ An encryption backdoor built into any of these becomes available to governments in other countries, notably the least trusted country.

3. “Going Dark” vs. a “Golden Age of Surveillance”⁷⁴

In terms of acceptance by other authors, our second key conclusion in the 2012 article has been more widely adopted than the first—we are not “Going Dark,” but instead are in a “Golden Age of Surveillance.”⁷⁵ In 2015 Senate testimony, Swire summarized the point in this way—that these specific law enforcement losses: “are more than offset by massive gains, including: (1) location information; (2) information about contacts and confederates; and (3) an array of new databases that create digital dossiers about individuals’ lives.”⁷⁶

The testimony specifically shows the enormous gains to law enforcement resulting from adoption in the past twenty years of

72. Swire & Ahmad, *supra* note 1, at 419.

73. For discussion of the same devices, software, and services, see RICHARD A. CLARKE, MICHAEL MORELL, GEOFFREY R. STONE, CASS R. SUNSTEIN & PETER SWIRE, PRESIDENT’S REV. GRP. ON INTEL. & COMM’NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT’S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES ch. 6, at 55 (2013).

74. Susan Landau originated the term “gold” in connection with the value of communication data. SUSAN LANDAU, SURVEILLANCE OR SECURITY? THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 99–104 (2011); see *Going Dark 2011 Hearing*, *supra* note 68, at 23 (statement of Susan Landau, Radcliffe Inst., Harv. Univ.).

75. For example, in 2014, technologist Bruce Schneier stated, “Fundamentally, we have reached the golden age of surveillance because we are all being surveilled ubiquitously.” Fahmida Y. Rashid, *Surveillance Is the Business Model of the Internet: Bruce Schneier*, SEC. WK. (Apr. 9, 2014), <https://www.securityweek.com/surveillance-business-model-internet-bruce-schneier/> [https://perma.cc/9VWZ-45EJ]; see Elaine McArdle, *The New Age of Surveillance*, HARV. L. TODAY (May 10, 2016), <https://hls.harvard.edu/today/new-age-surveillance/> [https://perma.cc/U495-XT72].

76. *Going Dark 2015 Hearing*, *supra* note 35, at 125.

digital smartphones and text messaging, the two areas most highlighted by law enforcement as examples of “going dark.” Although relatively few text messages were sent twenty years ago, by 2010 the number exceeded 6 trillion texts per year. For the predominant share of those messages, the content is available from the provider. Even for the subset where the content is encrypted, law enforcement can gain access to the meta-data, linking suspects and witnesses to their entire social graphs.

For text messages, it might be tempting to say that law enforcement could call the glass half-empty (some texts are encrypted) or half-full (some texts are in the clear). With over six trillion messages filling the cup, though, it takeschutzpah to say the glass is empty. Text messages are a prime example of a golden age of surveillance, and not of going dark.⁷⁷

Today, law enforcement and intelligence agencies have gained unprecedented access to new data sources, including facial recognition and AI search. When government agencies seek to limit encryption because they are “going dark,” it would appear even more true today that we live in a “golden age of surveillance.”⁷⁸

IV. ROUND 3: END-TO-END ENCRYPTION

Part IV discusses the current Round 3 of the Going Dark Debates, focused on issues of E2EE. We identify five distinct E2EE scenarios that reveal gaps between the assumption that E2EE prevents lawful access and the reality of how communications are actually sent and received. As in earlier rounds of the Going Dark debate, any proposed limitation on E2EE must be evaluated with the least trusted country in mind, as encryption broken for one government is broken for all.

A. Round 3 of the Going Dark Debates – Critiquing E2EE.

Round 2 of the Going Dark Debates, roughly from 2010 to 2015, focused on government concerns about encryption-in-transit, which blocked wiretaps from accessing content in the wide

77. *Id.*

78. *Accord* Rozenshtein, *supra* note 3, at 1200 (highlighting new potential sources of evidence for government such as from the Internet of Things, virtual and augmented reality, and large amounts of data accessible to technology companies for business reasons).

range of situations where encryption-in-transit became common. Law enforcement's response was to continue to rely on legal process to gain access to plaintext at the server—such as for Alice's or Bob's email provider—which remained effective because those providers could still read the content. There were also legal and policy battles about government access to a user's device—both physical access to a single device and remote access through software. This Article analyzes the latter, where third parties such as hackers or a government can gain access without having physical control of the user's device.⁷⁹

Round 3 focuses on government concerns about E2EE. As with Round 2, wiretaps are useless where there is encryption-in-transit. In addition, in Round 3, there is no entity between Alice and Bob who can read the plaintext. For what we call “true” or “implicitly assumed” versions of E2EE, legal process won't be able to access content from anyone other than Alice or Bob. With that said, there are other common and possible scenarios, where law enforcement may have access to content even when no entity between Alice and Bob is able to read the plaintext.

1. Significant But Far-From-Universal Rise in E2EE for Messaging

E2EE by default for messaging has increased significantly over time. Apple launched iMessage in 2011 with E2EE enabled between its iOS devices.⁸⁰ WhatsApp adopted E2EE by default in

79. There are potentially significant legal, policy, and technical differences between the government gaining access to content on a single device, such as after an arrest, and the government using software that may remotely access content on millions or billions of devices. This Article focuses on the latter. For discussion, see Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014) [hereinafter Bellovin et al., *Lawful Hacking*].

80. “When iMessage launched in 2011, it was the first widely available messaging app to provide end-to-end encryption by default.” SEAR, *iMessage with PQ3: The New State of the Art in Quantum-Secure Messaging at Scale*, APPLE SEC. RSCH. (Feb. 21, 2024), <https://security.apple.com/blog/imessage-pq3/> [https://perma.cc/EW64-D796]; Paul Sawers, *iPhone and Android Users Will Soon Be Able to Send Encrypted RCS Messages to Each Other*, TECHCRUNCH (Mar. 14, 2025), <https://techcrunch.com/2025/03/14/iphone-and-android-users-will-soon-be-able-to-send-encrypted-rcs-messages-to-each-other/> [https://perma.cc/Y3KB-FFDP]; see Zak Doffman, *RCS Encryption Is Nearly Here as Apple Changes iPhone*, FORBES (Apr. 8, 2026), <https://www.forbes.com/sites/zakdoffman/2026/04/08/stop-texting-apple-changes-iphone-after-15-years/> [https://perma.cc/ES38-6PGF] (discussing lengthy delay before E2EE availability for communications with

2016 for messages, calls, photos, and group chats.⁸¹ Signal uses E2EE by default for messaging, and grew from fewer than 1 million users in 2019 to 70 million active users by 2024.⁸² In 2023, Meta adopted E2EE as the global default for Messenger,⁸³ and Google did the same for Google Messages.⁸⁴ Other messaging services, such as Telegram, offer E2EE for messaging as an optional feature.⁸⁵

non-Apple devices). By 2012, iMessage had approximately 140 million users. Alexia Tsotsis, *iMessage Has More Than 140M Users and Has Sent Over 150B Messages, with Over 1B Messages Sent Per Day*, TECHCRUNCH (June 11, 2012), <https://techcrunch.com/2012/06/11/imessage-has-more-than-140m-users-and-has-150b-messages-over-1b-a-day/> [<https://perma.cc/3SND-7YM5>]. The approximate number of active monthly users in 2022 was 1.3 billion. Leonardo Pires, *iMessage Revenue and Growth Statistics (2024)*, SIGNHOUSE (Aug. 1, 2024), <https://usesignhouse.com/blog/imessage-stats/> [<https://perma.cc/MF9L-QSVX>].

81. Bill Budington, *WhatsApp Rolls Out End-to-End Encryption to Its Over One Billion Users*, ELEC. FRONTIER FOUND. (Apr. 7, 2016), <https://www.eff.org/deeplinks/2016/04/whatsapp-rolls-out-end-end-encryption-its-1bn-users> [<https://perma.cc/E5HD-B5UR>]; see Tonya Riley, *WhatsApp Adds End-to-End Encryption to Chat Backups, Locking Up Data in the Cloud*, CYBERSCOOP (Sept. 10, 2021), <https://cyberscoop.com/whatsapp-encryption-backup-chats/> [<https://perma.cc/5WUG-R5S3>]. At the time, the approximate number of monthly active users for WhatsApp was 1 billion. *Number of Monthly Active WhatsApp Users Worldwide from April 2013 to March 2025*, STATISTA (Nov. 25, 2025), <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/> [<https://perma.cc/HNM2-Q43F>]. The number of monthly active users as of 2025 is 3 billion. *Id.*

82. David Curry, *Signal Revenue & Usage Statistics (2026)*, BUS. APPS (Jan. 7, 2026), <https://www.businessofapps.com/data/signal-statistics/> [<https://perma.cc/636J-ZGLV>].

83. Loredana Crisan, *Launching Default End-to-End Encryption on Messenger*, META (Dec. 6, 2023), <https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/> [<https://perma.cc/7GEH-Y4MJ>]. “There are over 1.04 billion active users of Facebook Messenger worldwide in 2024, accounting for 30% of all mobile phone messaging app users globally.” Ash Turner, *Facebook Messenger Statistics: How Many People Use Facebook Messenger? (2026)*, BANKMYCELL (Apr. 8, 2024), <https://www.bankmycell.com/blog/number-of-facebook-messenger-users/> [<https://perma.cc/LD9Y-FC4K>].

84. GEC Admin Team, *Global Encryption Coalition Steering Committee Statement in Support of Industry Adoption of End-to-End Encryption*, GLOB. ENCRYPTION COAL. (Sept. 11, 2023), <https://www.globalencryption.org/2023/09/global-encryption-coalition-steering-committee-statement-in-support-of-industry-adoption-of-end-to-end-encryption/> [<https://perma.cc/H39K-KJ24>]. “Google reported that more than 1 billion active users use RCS in Messages every month.” Taras Mishchenko, *RCS in Google Messages Is Already Used by 1 Billion People, and the Company Is Preparing a Major Update in Honor of This*, MEZHA (Dec. 1, 2023), <https://mezha.ua/en/2023/12/01/rcs-in-google-messages-is-already-used-by-1-billion-people-and-the-company-is-preparing-a-major-update-in-honor-of-this/> [<https://perma.cc/9AYL-BZ68>].

85. Telegram does not use E2EE by default for its “Cloud Chats”; it does offer E2EE as a default for its “Secret Chats,” an optional encryption feature that is not part of the Telegram Cloud. *End-to-End Encryption FAQ*, TELEGRAM SUPPORT FORCE, <https://tsf.telegram.org/manuals/e2ee-simple> [<https://perma.cc/55N2-VKAF>] (last visited Mar. 10,

The adoption of E2EE by default has recently, and perhaps ironically, been encouraged by regulatory action. Text messages sent between iPhone and Android devices have historically lacked end-to-end encryption, even when messages within each platform were protected.⁸⁶ In March 2025, the GSMA—the industry body that sets mobile network standards worldwide—published Universal Profile 3.0, the specification for Rich Communication Services (RCS), the successor to SMS. For the first time it added end-to-end encryption requirements for cross-platform RCS messaging.⁸⁷ Apple and Google both announced their support, which means E2EE will be the default text-messaging channel between the two platforms that together represent more than ninety-nine percent of the global smartphone market.⁸⁸ Despite the European Union’s concerns about E2EE in other policy measures, a key driver of the GSMA standard was the EU Digital Markets Act,

2026); see Matthew Green, *Is Telegram Really an Encrypted Messaging App?*, FEW THOUGHTS ON CRYPTOGRAPHIC ENG’G (Aug. 25, 2024), <https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/> [https://perma.cc/W3QL-ARZZ] (“If you want to use end-to-end encryption in Telegram, you must manually activate an optional end-to-end encryption feature called ‘Secret Chats’ for every single private conversation you want to have”). Telegram reached 150 million users by 2017, and reportedly had 900 million users by 2024. Curry, *supra* note 82.

86. Doffman, *supra* note 80.

87. *GSMA RCS Universal Profile 3.0 Specifications*, GSMA (Mar. 13, 2025), https://www.gsma.com/solutions-and-impact/technologies/networks/gsma_resources/gsma-rcs-universal-profile-3-0-specifications/ [https://perma.cc/6E3W-4UMC]; see Tom Van Pelt, *RCS Encryption: A Leap Towards Secure and Interoperable Messaging*, GSMA (Mar. 14, 2025), <https://www.gsma.com/newsroom/article/rcs-encryption-a-leap-towards-secure-and-interoperable-messaging/> [https://perma.cc/8E6S-XQFJ]; see also Ravie Lakshmanan, *GSMA Confirms End-to-End Encryption for RCS, Enabling Secure Cross-Platform Messaging*, HACKER NEWS (Mar. 14, 2025), <https://thehackernews.com/2025/03/gsma-confirms-end-to-end-encryption-for.html> [https://perma.cc/UXX9-RP2C] [hereinafter *GSMA Confirms E2EE for RCS*].

88. Sawers, *supra* note 80. “Google and Apple have led a cross-industry effort to bring end-to-end encryption to Rich Communication Services (RCS), making the cross-platform messaging format that replaces traditional SMS more secure and private.” *End-to-End Encrypted RCS Messaging Begins Rolling Out Today for Android and iPhone Users*, GOOGLE: KEYWORD (May 11, 2026), <https://blog.google/products-and-platforms/platforms/android/android-ios-end-to-end-encrypted-rcs-messaging/> [https://perma.cc/2Z8C-TVBB]. The combined market share for Google’s Android and Apple’s iOS is approximately ninety-nine percent. *Mobile Operating System Market Share Worldwide, Mar 2025 – Mar 2026*, STATCOUNTER GLOB. STATS, <https://gs.statcounter.com/os-market-share/mobile/worldwide> [https://perma.cc/9ABS-Q6D6] (last visited Mar. 14, 2026); see *Mobile App Testing: 2026 iOS and Android Statistics*, PLUSQA, <https://www.plusqa.com/post/2026-ios-and-android-statistics> [https://perma.cc/Y572-MUY4] (last visited Mar. 10, 2026).

which requires large technology platforms to ensure interoperability with rival services.⁸⁹

At the same time, other developments have reduced the prevalence of E2EE for messaging. In March 2026, Meta announced that E2EE direct messaging on Instagram would no longer be supported, citing low adoption.⁹⁰ TikTok, which has never offered E2EE for its direct messages,⁹¹ grew from roughly 300 million active users in 2018 to over 2 billion users by early 2026.⁹² Some governments have acted against E2EE directly. China has blocked E2EE apps such as Signal.⁹³ Russia has similarly blocked E2EE apps citing anti-terrorism and data-localization requirements.⁹⁴ Many

89. Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), 2022 O.J. (L 265) 1; *see GSMA Confirms E2EE for RCS*, *supra* note 87; Mallory Knodel, *A Playbook for End-to-End Encrypted Messaging Interoperability*, TECHPOLICY.PRESS (Jan. 24, 2025), <https://www.techpolicy.press/a-playbook-for-endtoend-encrypted-messaging-interoperability/> [<https://perma.cc/FP36-UT5A>].

90. Ravie Lakshmanan, *Meta to Shut Down Instagram End-to-End Encrypted Chat Support Starting May 2026*, HACKER NEWS (Mar. 13, 2026), <https://thehackernews.com/2026/03/meta-to-shut-down-instagram-end-to-end.html> [<https://perma.cc/4DBD-AHGM>]. The company had never made E2EE the default for the app's chat (i.e., direct messaging) function, rolled it out fully, or promoted it within the app. *Id.*; *see The Real Reason Meta Dropped Instagram Encryption*, CYBER SAFETY GUY (Apr. 13, 2026), <https://www.cybersafetyguy.com/p/the-real-reason-meta-dropped-instagram> [<https://perma.cc/AM5F-ZNHQ>].

91. Joe Tidy, *TikTok Won't Protect DMs with Controversial Privacy Tech, Saying It Would Put Users at Risk*, BBC NEWS (Mar. 3, 2026), <https://www.bbc.com/news/articles/cly2m5e5ke4o> [<https://perma.cc/NJ3Q-3DRL>].

92. *The Rapid Rise of TikTok: Chart*, STATISTA, <https://www.statista.com/chart/28412/social-media-users-by-network-amo/> [<https://perma.cc/Q5TG-7C89>] (last visited Mar. 10, 2026); Robert A. Lee, *TikTok Usage Statistics 2026: User Growth, Engagement, and More*, SQ MAG. (Feb. 5, 2026), <https://sqmagazine.co.uk/tiktok-usage-statistics/> [<https://perma.cc/AK6Q-AVWC>] (estimating 21.7 percent of TikTok users use the app's direct messaging function).

93. Associated Press, *Signal: China Appears to Have Blocked Encrypted Messaging App*, GUARDIAN (Mar. 16, 2021), <https://www.theguardian.com/world/2021/mar/16/signal-blocked-china-encrypted-messaging-app> [<https://perma.cc/27M2-TF2P>]; Valentin Weber, *How China's Control of Information Is a Cyber Weakness*, LAWFARE (Nov. 12, 2020), <https://www.lawfaremedia.org/article/how-chinas-control-information-cyber-weakness> [<https://perma.cc/59X5-4TAY>]; Laskai & Segal, *supra* note 71. In 2023, India banned fourteen specialized messaging apps, which utilized E2EE, citing to concerns that terrorists utilized these apps. Jyoti Panday, *Encryption Under Siege in India: National Security & the Erosion of Digital Privacy*, INTERNET GOVERNANCE PROJECT (Oct. 20, 2024), <https://www.internetgovernance.org/2024/10/20/encryption-under-siege-in-india-national-security-the-erosion-of-digital-privacy/> [<https://perma.cc/B2PG-D3YA>].

94. Dasha Litvinova, *Russia Restricts FaceTime in Latest Step to Control Online Communications*, PBS NEWS (Dec. 4, 2025), <https://www.pbs.org/newshour/world/>

messages are sent through enterprise software services such as Google Workspace (Google Chat), Microsoft Teams, and Slack, which do not use E2EE by default.⁹⁵ As a factual matter, therefore, a substantial fraction of messaging is not currently protected by E2EE by default.

2. From Jawboning to Proposed Legal Limits on E2EE

In Round 3 of the Going Dark Debate, in response to the growth of E2EE, there have been numerous proposals in the United States, European Union, and elsewhere to limit use of E2EE.⁹⁶ Only a small subset of these proposals, however, have been adopted.⁹⁷

As with previous rounds of the Going Dark Debates, law enforcement and intelligence agencies have been leading critics of risks from new encryption adoption. One prominent example is the 2020 press release, “International Statement: End-To-End Encryption and Public Safety,” signed by the US Attorney General, counterpart officials from the other “Five Eyes” countries—Australia, Canada, New Zealand, and the United Kingdom—and the governments of India and Japan.⁹⁸ The statement highlighted the risks of E2EE in messaging, and urged technology companies to take steps to “[e]nable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight.”⁹⁹ The emphasis on “access to content in

russia-restricts-facetime-in-latest-step-to-control-online-communications [https://perma.cc/UJT5-UBL9]; *Massive Blocking Campaign in Russia: What You Need to Know for Private Communication*, PROTECTSTAR (Sept. 20, 2024), https://www.protectstar.com/en/blog/blocking-campaign-russia [https://perma.cc/ZT3H-5XU6].

95. In 2024, Microsoft Teams had 320 million users. David Curry, *Microsoft Teams Revenue and Usage Statistics (2026)*, BUS. APPS (Jan. 7, 2026), https://www.businessofapps.com/data/microsoft-teams-statistics/ [https://perma.cc/VL3P-MP6M].

96. Marcin Rojszczak, *End-to-End Encryption, Chat Control, and the Future of the Right to Encryption in Digital Services*, 12 J. CYBERSECURITY 1 (2026), https://academic.oup.com/cybersecurity/article/12/1/tyag010/8677339 [https://perma.cc/2JBH-KUYZ].

97. Thorin Klosowski, *Defending Encryption in the U.S. and Abroad: 2025 in Review*, ELEC. FRONTIER FOUND. (Dec. 28, 2025), https://www.eff.org/deeplinks/2025/12/defending-encryption-us-and-abroad-2025-review [https://perma.cc/7ZJA-97CQ].

98. Press Release, U.S. Dep’t of Just., International Statement: End-to-End Encryption and Public Safety (Oct. 11, 2020), https://www.justice.gov/archives/opa/pr/international-statement-end-end-encryption-and-public-safety [https://perma.cc/MTH4-B5TR].

99. *Id.*

a readable and usable format” directly targets the possible lack of such access with E2EE messaging.

This statement had no legally binding status. However, one can view it, and similar statements, as “jawboning,” “when the government pressures private entities, often through public speech or behind-the-scenes conversations, to take certain actions.”¹⁰⁰ The United States and other governments have also pressured private companies to refrain from deploying E2EE.¹⁰¹

Beyond jawboning, Australia and the United Kingdom have enacted two noteworthy laws to restrict E2EE. Australia’s Assistance and Access Act 2018 established a framework for requiring industry providers to offer technical assistance to law enforcement and intelligence agencies.¹⁰² The United Kingdom’s Online Safety Act 2023 authorizes regulators to require platforms to maintain technical access to encrypted content.¹⁰³ The United Kingdom’s Investigatory Powers Act 2016 authorizes the Home Secretary to issue Technical Capability Notices requiring telecommunications operators to maintain the capability to provide access to communications, including by removing electronic protection. As discussed in Scenario 2 below, the UK issued such a notice to Apple, requiring that legal process remain

100. Frances Badgett, *One Quick Question: What Are the Origins of the Term “Jawboning”?*, W. WASH. UNIV. NEWS (Oct. 3, 2025), <https://news.wvu.edu/one-quick-question-what-is-the-origin-of-jawboning-and-how-does-it-relate-to-freedom-of-speech> [<https://perma.cc/CRJ4-YYM7>]. “[A]ttempts by government actors to influence private action by threat of future regulation can be considered coercive.” VALERIE C. BRANNON & WHITNEY K. NOVAK, CONG. RSCH. SERV., LSB10742, ONLINE CONTENT MODERATION AND GOVERNMENT COERCION 2 (2022). For a critique of the practice of jawboning, see Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51 (2015).

101. Press Release, U.S. Dep’t of Just., Off. of Pub. Affs., Attorney General Barr Signs Letter to Facebook from US, UK, and Australian Leaders Regarding Use of End-to-End Encryption (Oct. 3, 2019), <https://www.justice.gov/archives/opa/pr/attorney-general-barr-signs-letter-facebook-us-uk-and-australian-leaders-regarding-use-end> [<https://perma.cc/E8JA-NRPH>].

102. *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (Austl.); see Taylor Rajic, *Revisiting Australia’s Encryption Landscape*, CTR. FOR STRATEGIC & INT’L STUD. (Aug. 20, 2024), <https://www.csis.org/blogs/strategic-technologies-blog/revisiting-australias-encryption-landscape> [<https://perma.cc/MES8-6MX8>].

103. Online Safety Act 2023, c. 50 (UK); see *The UK Online Safety Bill: A Massive Threat to Online Privacy, Security, and Speech*, ELEC. FRONTIER FOUND. (Sept. 19, 2023), <https://www.eff.org/pages/uk-online-safety-bill-massive-threat-online-privacy-security-and-speech> [<https://perma.cc/S5CG-B9HD>].

effective for government access to iCloud content.¹⁰⁴ In 2025¹⁰⁵ and 2026,¹⁰⁶ Canada considered legislation giving law enforcement access to encrypted communications and allowing secret government orders to telecom companies, potentially requiring backdoors into encrypted networks. These proposals have drawn sharp opposition, notably for the risks to digital security from mandated backdoors in E2EE.¹⁰⁷

In the United States, similar legislation has been proposed in Congress—primarily out of concern about child sexual abuse material (CSAM)—but has not been enacted.¹⁰⁸ One prominent example is the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act which seeks to impose accountability, to eliminate specific statutory protections for service providers that have CSAM on their sites.¹⁰⁹ As described by the Internet Society in 2022, “[t]he EARN IT Act threatens a company’s ability to use and offer end-to-end encryption by putting their liability immunity at risk if they do not proactively

104. See *infra* Part IV.B.2.

105. Tamir, *Government Needs to Fix Dangerous Flaws in Federal Cybersecurity Proposal*, CAN. C.L. ASS’N (Sept. 26, 2025), <https://ccla.org/privacy/fix-dangerous-flaws-in-federal-cybersecurity-proposal/> [https://perma.cc/X7FD-VUBJ].

106. Bill C-22, An Act Respecting Lawful Access, 1st Sess., 45th Parl. (Can. 2026) (first reading Mar. 12, 2026).

107. *A Tale of Two Bills: Lawful Access Returns with Changes to Warrantless Access But Dangerous Backdoor Surveillance Risks Remain*, MICHAEL GEIST (Mar. 13, 2026), <https://www.michaelgeist.ca/2026/03/a-tale-of-two-bills-lawful-access-returns-with-changes-to-warrantless-access-but-dangerous-backdoor-surveillance-risks-remains/> [https://perma.cc/L64X-TZYF]; *Canada’s Encryption Proposal Would Undermine Digital Security*, INFO. TECH. & INNOVATION FOUND. (Mar. 12, 2026), <https://itif.org/publications/2026/03/12/canadas-encryption-proposal-would-undermine-digital-security/> [https://perma.cc/GF52-VCY3]; *Apple and Google Warn Canadian Encryption Bill Could Weaken User Security*, HACK ACAD. (May 27, 2026), <https://www.thehackacademy.com/news/apple-and-google-warn-canadian-encryption-bill-could-weaken-user-security/> [https://perma.cc/4FQE-VC5F]; Ryan Polk, *Open Letter on Bill C-22, An Act Respecting Lawful Access*, GLOB. ENCRYPTION COAL. (Apr. 28, 2026), <https://www.globalencryption.org/2026/04/open-letter-on-bill-c-22-an-act-respecting-lawful-access/> [https://perma.cc/H8KX-4K4T].

108. See Klosowski, *supra* note 97; Tom Bowman, *The STOP CSAM Act Would Make Kids Less Safe*, CTR. FOR DEMOCRACY & TECH. (June 13, 2025), <https://cdt.org/insights/the-stop-csam-act-would-make-kids-less-safe/> [https://perma.cc/F5FP-DWY5]; see also EARN IT Act of 2023, S. 1207, 118th Cong. (2023); *Privacy’s Best Friend: Encryption Debates in Congress*, NEW AM. (Aug. 24, 2020), <https://www.newamerica.org/insights/privacy-best-friend/encryption-debates-in-congress/> [https://perma.cc/T6YT-DGP4].

109. Press Release, S. Comm. on the Judiciary, Graham, Blumenthal Reintroduce EARN IT Act (Apr. 19, 2023), <https://www.judiciary.senate.gov/press/rep/releases/graham-blumenthal-reintroduce-earn-it-act/> [https://perma.cc/W7MY-7DUU].

monitor and filter for illegal user content.”¹¹⁰ Although passed out of committee, it was not enacted. Other proposed US legislation that might threaten E2EE, supported in the name of reducing CSAM, includes the STOP CSAM Act of 2023 and the Kids Online Safety Act (KOSA).¹¹¹

In the European Union, the European Commission published a Roadmap for Effective and Lawful Access to Data for Law Enforcement in 2025.¹¹² The Roadmap announced that the Commission will present a Technology Roadmap on Encryption to “identify and evaluate solutions that enable lawful access to encrypted data by law enforcement, while safeguarding cybersecurity and fundamental rights,” and will support the development of next-generation decryption capabilities for Europol by 2030.¹¹³ Measures “that enable lawful access” or constitute “next-generation decryption capabilities” would appear to challenge use of E2EE.

In opposition to these proposals and new laws restricting E2EE, there have been striking instances of government support for E2EE, including from the FBI. In 2024, Chinese state-sponsored hackers were discovered to have compromised the wiretap systems that major US telecommunications carriers had built to comply with US law,¹¹⁴ in a campaign that became known as Salt

110. Natalie Campbell et al., *Internet Impact Brief: How the US EARN IT Act Threatens Security, Confidentiality, and Safety Online*, INTERNET SOC'Y (Nov. 17, 2022), <https://www.internetsociety.org/resources/2022/internet-impact-brief-how-the-us-earn-it-act-threatens-security-confidentiality-and-safety-online/> [https://perma.cc/W2PM-3QZ7].

111. Allison Cross, *Speak Out Against Bills That Threaten End-to-End Encryption*, INTERNET SOC'Y (June 14, 2023), <https://www.internetsociety.org/blog/2023/06/speak-out-against-bills-that-threaten-end-to-end-encryption/> [https://perma.cc/UH89-SCR3].

112. Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Roadmap for Lawful and Effective Access to Data for Law Enforcement, COM (2025) 349 final (June 24, 2025).

113. *Id.*; see Directorate-General for Migration & Home Affs., *Commission Presents Roadmap for Effective and Lawful Access to Data for Law Enforcement*, EUR. COMM'N (June 24, 2025), https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en [https://perma.cc/S6P6-TKZ2].

114. The carriers had built wiretap systems to comply with the Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001–1010). For a history of CALEA and its role in US wiretaps, see Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Going Bright: Wiretapping Without Weakening Communications Infrastructure*, 11 IEEE SEC. & PRIV. 62 (2013)

Typhoon.¹¹⁵ The attackers accessed real-time phone calls of targeted individuals, phone metadata for the Washington, D.C. area, and the systems used to process law enforcement surveillance requests.¹¹⁶ In December 2024, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) responded by urging Americans to use end-to-end encrypted messaging, with a CISA official stating publicly that “encryption is your friend.”¹¹⁷

As discussed further below, along with this support from government agencies for E2EE, criticisms of limits on E2EE came once again from a coalition of privacy supporters, online commerce providers, and cybersecurity experts.¹¹⁸ Our discussion here supplements those contributions by explaining important practical features of how E2EE is deployed, and how that tends to undermine government claims of the need to break E2EE.

[hereinafter Bellovin et al., *Going Bright*]. See *CALEA Background*, CTR. FOR DEMOCRACY & TECH. (Sept. 28, 2010), <https://cdt.org/insights/calea-background/> [<https://perma.cc/PCF7-PA5E>]; *CALEA: FAQ on the FCC CALEA Expansion*, ELEC. FRONTIER FOUND., <https://www.eff.org/issues/calea> [<https://perma.cc/7F62-7AJA>] (last visited Mar. 10, 2026).

115. Sarah Krouse et al., *China-Linked Hackers Breach U.S. Internet Providers in New ‘Salt Typhoon’ Cyberattack*, WALL ST. J. (Sept. 26, 2024), <https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835> [<https://perma.cc/G4KL-UBGW>]; see CHRIS JAIKARAN, CONG. RSCH. SERV., IF12798, SALT TYPHOON HACKS OF TELECOMMUNICATIONS COMPANIES AND FEDERAL RESPONSE IMPLICATIONS (2025) [hereinafter SALT TYPHOON HACKS].

116. Kevin Collier, *Telecoms Haven’t Notified Most Victims of Chinese Phone Data Hacking Campaign, Sources Say*, NBC NEWS (Dec. 12, 2024), <https://www.nbcnews.com/tech/security/phone-hack-data-chinese-salt-typhoon-metadata-fbi-security-encryption-rcna183233> [<https://perma.cc/YJS6-MZVG>]; Andres Triay, Robert Legare & Kathryn Watson, *The U.S. Is Investigating a China-Backed Hack of Telecom Companies. Here’s What to Know*, CBS NEWS (Oct. 11, 2024), <https://www.cbsnews.com/news/us-investigating-hack-major-telecom-companies-by-china/> [<https://perma.cc/R7V8-U3HH>]; see also SALT TYPHOON HACKS, *supra* note 115 (confirming reports that hackers targeted systems used to provide court-approved access to communications for law enforcement and intelligence investigations).

117. Bill Chappell, *FBI Warns Americans to Keep Their Text Messages Secure: What to Know*, NPR (Dec. 17, 2024), <https://www.npr.org/2024/12/17/nx-s1-5223490/text-messaging-security-fbi-chinese-hackers-security-encryption> [<https://perma.cc/5RWP-DXNZ>] (quoting Jeff Greene, CISA’s executive assistant director for cybersecurity, stating “Encryption is your friend”). Notably, CALEA “help[ed] law enforcement maintain its ability to execute authorized electronic surveillance Telecommunications carriers [were] not responsible for decrypting any encrypted communications.” *LAWFUL ACCESS DEBATE*, *supra* note 19.

118. See *infra* Parts V.B, V.C.

B. The Technical Diagrams: Five Variations for End-to-End Encryption in Messaging

The term “end-to-end encryption” covers more scenarios than the simple model that policymakers may implicitly assume. In the simple model, Alice sends a message to Bob. The message is encrypted on Alice’s device and decrypted on Bob’s device. No one in between—not the network operator, nor the service provider—can read it. For this simple and implicitly assumed model, only access to Alice’s or Bob’s device can give another access to the plaintext.

The problem, however, is in determining what constitutes the “ends” in any given system. Scholars Chelsea Komlo and Britta Hale were the first to formally define and explore the concept of “endness,” referring to the defined “ends” or endpoints that can access plaintext.¹¹⁹ To visualize the concept, assume Alice sends an E2EE message to Bob and Bob opens it in a cloud-based application, which is often called “software as a service” (SaaS).¹²⁰ The message is encrypted by Alice, and no one can read the plaintext between the moment it leaves Alice and the moment it reaches its destination. Crucially, however, given how Bob opens the message (at his “endpoint”), the plaintext may be available both to Bob and to the SaaS provider. That is, there is E2EE, but the way the message “ends” for Bob may make the plaintext available to the SaaS provider. This example is further developed as Scenario 3 below. Each of the five scenarios that follow will reflect different “ends,” that is, what qualifies as an end and what access that end permits.

We will now identify five technically distinct scenarios for the recipient “end” of an encrypted communication, each with different implications for law and policy: (1) the simple or implicitly-assumed model, where access is available only with access to the device of Alice and Bob; (2) cloud backup access, where encrypted content is stored in a backup the provider can read; (3) SaaS or other server-side access, where the provider

119. Britta Hale & Chelsea Komlo, *On End-to-End Encryption* (Cryptology ePrint Archive, Paper No. 2022/449, 2022), <https://eprint.iacr.org/2022/449> [<https://perma.cc/RM97-TKPN>]; see Harold Abelson et al., *Bugs in Our Pockets: The Risks of Client-Side Scanning*, 10 J. CYBERSECURITY 1 (2024) [hereinafter Abelson et al., *Bugs in Our Pockets*].

120. Hale & Komlo, *supra* note 119, at 7.

holds keys or plaintext at some point in the process; (4) on-device scanning, where content is analyzed on the user's device before encryption or after decryption; and (5) ghost protocol, where a silent participant, such as a government agency, is added to the conversation and can receive messages without the other parties knowing. In practice, scenarios (2) and (3) are especially common, resulting in messages sent with E2EE but eventually subject to law enforcement access.

1. Scenario 1: "True" or "implicitly assumed" E2EE.

Diagram 3A illustrates what we call the "true" or "implicitly assumed" scenario for E2EE messaging. As with all five scenarios, the communication is encrypted in transit, blocking wiretaps and any other man-in-the-middle attacks. As with all scenarios, the messaging app enables communication without that app itself having access to the plaintext.

If the government wishes to gain access to the plaintext, its options are strictly limited. First, Alice or Bob might reveal the messages themselves, such as if the government asks Bob or Bob complies with legal process. Second, the government might access the device of Alice or Bob: either Alice or Bob grants the government access to their device, such as by providing a passcode or providing a biometric identifier, or the government seizes the device and finds some way to open it and read the plaintext without assistance from Alice or Bob.

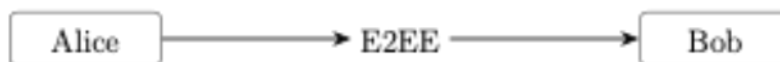


Diagram 3A: "True" E2EE

It is worth emphasizing that there can be terminological confusion about whether only this scenario qualifies as E2EE. System designers, cryptographers, and users may implicitly assume that *only* this scenario matches the term. As discussed, next, however, other common scenarios leverage E2EE in *some* part of the messaging scheme so that no entity between Alice and Bob can access the content, but still allow for lawful access via some additional step in their infrastructure. This Article uses the

term “E2EE” in the broader sense, where no entity between Alice and Bob can access the content.

2. Scenario 2: The Government Can Access Content that the Device Uploads to the Cloud.

Diagram 3B illustrates how content that reaches Bob’s device may be backed up to the cloud. In this scenario, the message is encrypted from Alice to Bob’s device. Bob’s device, however, then backs up the content in the cloud, by Bob’s choice or as a default setting, potentially allowing the cloud provider access. There are many reasons in modern computing why this backup may occur. For instance, Bob may wish to have an extra copy of his content in case he loses a device. In addition, backup to the cloud enables up-to-date access by Bob through any of his multiple devices.¹²¹

One important factor in whether the government can gain access in this scenario is whether Bob’s backup is encrypted in a form so that he only holds the key or whether the cloud provider also holds a key. Where only Bob holds the key, the backup is unreadable to the provider, and legal process served on the provider cannot yield the plaintext. Where the provider holds a key, it can. In the United States and other countries, for instance, Apple offers an opt-in feature called “Advanced Data Protection” (ADP).¹²² ADP uses E2EE between Bob and the iCloud backup—Apple cannot access Bob’s data, and the keys remain only on the devices that Bob selects.¹²³

121. See *What Is Cloud Backup & Disaster Recovery: Best Practices & Solutions*, DATABANK (Nov. 10, 2025), <https://www.databank.com/resources/blogs/what-is-cloud-backup-disaster-recovery-best-practices-solutions/> [<https://perma.cc/S2DQ-R5X9>]; Joe Aucott, *10 Reasons You Should Be Using Cloud Backup for Effective Disaster Recovery*, HAPTIC (July 17, 2023), <https://haptic-networks.com/cloud/10-reasons-for-cloud-backup-services/> [<https://perma.cc/M8QH-WB8R>]; *Importance of Cloud Backup When Saving Files*, NORDICBACKUP, <https://nordic-backup.com/blog/importance-of-cloud-backup-when-saving-files/> [<https://perma.cc/62WH-P6NE>] (last visited Mar. 14, 2026); see also *How Technology Helped Ukraine Resist During Wartime*, MICROSOFT (Jan. 20, 2023), <https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/> [<https://perma.cc/U6CJ-6FTA>] (explaining how Ukraine’s government backed up data to the cloud to allow it to remain functioning during wartime).

122. *iCloud Data Security Overview*, APPLE SUPPORT (Jan. 5, 2026), <https://support.apple.com/en-us/102651> [<https://perma.cc/GQA2-VY2C>].

123. *Id.*; *How to Turn on Advanced Data Protection for iCloud*, APPLE SUPPORT (Sept. 26, 2024), <https://support.apple.com/en-us/108756> [<https://perma.cc/6VZ7-NR3A>].

Following a notice served by the UK government under the Investigatory Powers Act, however, Apple no longer offers iCloud backup with ADP in the United Kingdom.¹²⁴ Bob's iCloud data remains encrypted in transit to iCloud and encrypted at rest in iCloud. Apple, however, retains keys that can access most content under standard protection. Messages in iCloud are also E2EE, but that protection no longer applies once iCloud Backup is enabled by default.¹²⁵ Note that an individual in the United States uses the non-ADP form of iCloud backup by default—that way, if the individual loses their key, they don't lose access to their iCloud content. For purposes of understanding Scenario 2, however, the main point is that there was E2EE between Alice and Bob, but in the absence of ADP the backup is readable by someone other than Bob.¹²⁶



Diagram 3B: Government Can Access Content That Is Backed Up to the Cloud

3. Scenario 3: The Government Can Access Content through Software as a Service.

Diagram 3C illustrates the SaaS scenario mentioned above.¹²⁷ Once again, E2EE is present from “end” one, Alice, until Bob opens the communication at “end” two—no wiretap or man-in-the-middle attack will succeed between the two points. The important difference here is that Bob opens the message content in a SaaS environment—that is, in a form where the SaaS provider can

124. *Apple Can No Longer Offer Advanced Data Protection in the United Kingdom to New Users*, APPLE SUPPORT (Sept. 22, 2025), <https://support.apple.com/en-us/122234> [<https://perma.cc/57WC-MCCH>]; see Bill Goodwin, *Home Office Issues New ‘Backdoor’ Order Over Apple Encryption*, COMPUT. WKLY. (Oct. 1, 2025), <https://www.computerweekly.com/news/366632159/Home-Office-issues-new-back-door-order-over-Apple-encryption> [<https://perma.cc/4LRF-PBPR>]; see also Susan Landau, Matt Blaze & Steven M. Bellovin, *The U.K.’s Plan for Electronic Eavesdropping Poses Cybersecurity Risks*, LAWFARE (Jan. 8, 2026), <https://www.lawfaremedia.org/article/the-u.k.-s-plan-for-electronic-eavesdropping-poses-cybersecurity-risks> [<https://perma.cc/EHF4-ZVYG>].

125. *iCloud Data Security Overview*, *supra* note 122. Fifteen categories, including Health, are E2EE under standard protection. Messages in iCloud is E2EE only when iCloud Backup is off; when Backup is on (the default), Apple can access it via the backup key. *Id.*

126. Scenario 2, with back-up in the cloud, differs from Scenario 4. In Scenario 4, content may be stored only on Bob’s device, and not backed up to the cloud.

127. See *supra* Part IV.B.

access the content. With such access, the SaaS provider can be compelled to produce the content, just as the iCloud provider could be reached and compelled in scenario 2.

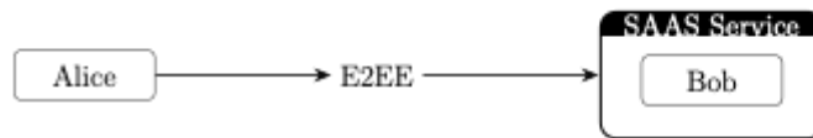


Diagram 3C: Government Can Access Through SaaS

SaaS is generally defined as cloud-based software delivered over the Internet from the provider's servers rather than installed locally on the user's device.¹²⁸ SaaS has become the dominant model for both consumer and enterprise computing, increasingly displacing content storage on an individual's device.¹²⁹ The enterprise market relies on prominent SaaS business services such as Workday and Salesforce, and an estimated eighty-five percent of business apps are now SaaS-based.¹³⁰ Businesses and individuals both widely use subscription SaaS services for messaging and content sharing, including through the SaaS providers discussed above.¹³¹ Large numbers of individuals also access free SaaS solutions such as Gmail (over 1.5 billion users per month) and Google Docs (over 1 billion users per month).¹³²

The SaaS model shows the importance of defining different scenarios for "endness." By Round 2 of the Going Dark debate,

128. *What Is Software as a Service (SaaS)?*, MICROSOFT AZURE, <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas> [https://perma.cc/N2PD-XMPZ] (last visited Mar. 10, 2026).

129. "SaaS has become the dominant software model in the 21st century because it helps companies operate with increased ease, intelligence, and quality." *What Is SaaS (Software as a Service)?*, SALESFORCE, <https://www.salesforce.com/saas/> [https://perma.cc/VVF5-PDZL] (last visited Mar. 10, 2026); see Jocelyn Ho, *60+ Eye-Opening SaaS Statistics (2025)*, SPENDESK (Mar. 12, 2026), <https://www.spendsk.com/blog/saas-statistics/> [https://perma.cc/KGG8-NL77].

130. Ho, *supra* note 129. Microsoft 365 and Google Workspace together have over ninety percent of the business user market. Lauren Ballejos, *Google Workspace vs. Microsoft 365: Which One Is Best for Businesses?*, NINJAONE (Sept. 2, 2025), <https://www.ninjaone.com/blog/google-workspace-vs-microsoft-365/> [https://perma.cc/4JPC-R9U7].

131. Ho, *supra* note 129.

132. *Key Google Workspace Statistics for 2025*, PATRONUM (Apr. 26, 2023), <https://www.patronum.io/key-google-workspace-statistics-for-2023> [https://perma.cc/7G8A-QJYD].

around 2012, cloud storage for email had become important enough that government access to such cloud storage was a crucial tool for lawful access. Today, SaaS plays the same role on a larger scale: local storage on a single device accounts for a decreasing share of overall computing, and the dominant role of SaaS means that a correspondingly large portion of communications, content sharing, and other online files are available through lawful access to the SaaS provider. The evolution of computing thus once again produces a “golden age of surveillance” for government agencies that use lawful access. Even E2EE does not block lawful access, if Bob opens the communication within a SaaS environment.

4. Scenario 4: Software on the Device Can Give Access to the Government.

Diagram 3D illustrates how software may reside on the device of Alice or Bob, and that software may provide access to the government. Scenario 4 does involve E2EE as the term is used in this Article—the communication is encrypted in transit, blocking wiretaps or any other man-in-the-middle attacks. As with all scenarios, the messaging app enables communication without the app itself having access to the plaintext. Here, however, software on Bob’s device—whether spyware or a feature of the device’s own operating system—makes the plaintext available to a third party in the process of Bob opening the message on his device. Because this other software has access to the plaintext once the communication arrives to Bob’s device, lawful government access of its content would be technologically possible.

Such software may be on Bob’s device from some form of exploit, or it may be built into software already present on the device, such as the operating system. The first route is illustrated by spyware such as Pegasus, sold by the company NSO Group, which has been the subject of extensive public reporting.¹³³ NSO

133. “The investigation by the Guardian and 16 other media organisations suggests widespread and continuing abuse of NSO’s hacking spyware, Pegasus, which the company insists is only intended for use against criminals and terrorists.” Stephanie Kirchgaessner et al., *Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon*, GUARDIAN (July 18, 2021), <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus> [<https://perma.cc/L4T2-HVCT>]. “[T]he Citizen Lab, a University of Toronto-based research group that undertakes evidence-based research on targeted digital espionage, . . . identified hundreds of people whose phones have been targeted or hacked . . .” Ron Deibert, *Protecting Society from*

Group and other spyware providers sell surveillance tools to governments, who deploy them against targets. Once installed on Bob's device via an exploit, the spyware can read the plaintext and transmit it to the government agency using it.

Monitoring or scanning software can exist on Bob's device, using no exploit at all via the second route. For example, in 2021 Apple proposed a plan to include software in iOS that would scan photos on user devices for CSAM; when detected, the operating system would send a report to Apple or an entity designated by Apple.¹³⁴ Had it launched, this would have given Apple direct access to flagged content on Bob's device, with no exploit needed. Apple's plan was met with fierce backlash from privacy and security experts, and the system was never actually deployed.¹³⁵

Scenario 4 differs from the others: the path to the plaintext runs through the device itself, not a backup, provider, or communication in transit. Whether by exploit or by design, software at an "end" can expose content encryption otherwise protects, another example of how "endness" determines who ultimately gets the plaintext.



Surveillance Spyware, 38 ISSUES IN SCI. & TECH. 15, 15 (2022); see John Scott-Railton et al., *New Pegasus Spyware Abuses Identified in Mexico*, CITIZEN LAB (Oct. 2, 2022), <https://citizenlab.ca/research/new-pegasus-spyware-abuses-identified-in-mexico/> [https://perma.cc/T3GQ-JMH7]; John Scott-Railton et al., *GeckoSpy: Pegasus Spyware Used Against Thailand's Pro-Democracy Movement*, CITIZEN LAB (July 17, 2022), <https://citizenlab.ca/research/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/> [https://perma.cc/HJ8U-UM6T]; Ron Deibert, *UK Government Officials Infected with Pegasus*, CITIZEN LAB (Apr. 18, 2022), <https://citizenlab.ca/research/uk-government-officials-targeted-pegasus/> [https://perma.cc/T44G-UZZC].

134. Julian Sanchez, *Apple's iPhone: Now With Built-In Surveillance*, CATO INST. (Aug. 6, 2021), <https://www.cato.org/blog/apples-iphone-now-built-surveillance> [https://perma.cc/E2C5-CZGF].

135. Julian Sanchez, *After Backlash, Apple Postpones Photo Scanning Plans*, CATO INST. (Sept. 14, 2021), <https://www.cato.org/blog/after-backlash-apple-postpones-photo-scanning-plans-0> [https://perma.cc/JK6D-CXC4]; see Abelson et al., *Bugs in Our Pockets*, *supra* note 119.

Diagram 3D: Software on the Device Can Give Access to Government

5. Scenario 5: “Ghost” and Group Chats.

Diagram 3E illustrates ghost protocol. The idea was to silently add a government participant to an encrypted conversation. Diagram 3E shows a group chat, where Alice sends an E2EE encrypted message to recipients Bob, Charles, Deirdre, Ellen, and Frank. Government access occurs in this scenario because the message goes to an additional recipient, the “Ghost” or “Government,” without the knowledge of others in the group chat.¹³⁶

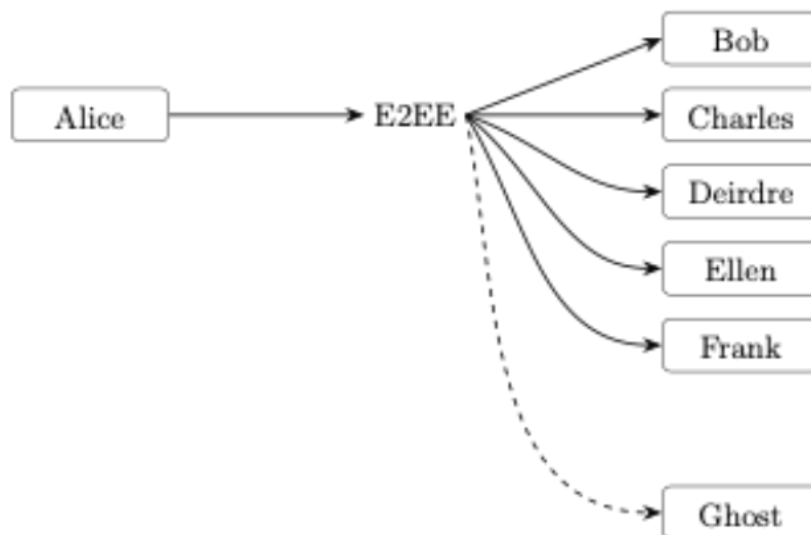


Diagram 3E: The Ghost Protocol

The ghost protocol proposal qualifies as E2EE, as defined in this Article, because Alice sends an E2EE message to Bob (and other recipients) without any wiretap or man-in-the-middle attack. The encryption process of the message from Alice’s end is not compromised. What changes is the definition of endness: who is treated as an endpoint. Although the mathematics of encryption

136. The protocol could also work to add the Ghost recipient to a message otherwise only going from Alice to Bob.

still operate effectively between Alice and Bob, government access is achieved by manipulating the messaging system's authorization architecture, specifically by changing which parties the system treats as authorized recipients. The practical effect is that the user believes they are communicating privately when they are not.¹³⁷

In 2018, officials from Government Communications Headquarters (GCHQ), the United Kingdom's signals intelligence agency, proposed what has come to be known as "ghost protocol." The proposal generated substantial opposition.¹³⁸ In May 2019, forty-seven organizations including Apple, Google, Microsoft, and WhatsApp published an open letter arguing that ghost protocol would undermine user trust and create serious security risks.¹³⁹ The proposal has not been implemented but remains a useful illustration of how the concept of endness can be manipulated so that the government or other third parties can gain access to otherwise encrypted plaintext. Therefore, again, the policy question is not only about the strength of encryption but about how systems define and manage their endpoints.

C. E2EE Protects Confidentiality for Far More Than Messaging.

Sub-part B showed that there are important E2EE messaging scenarios beyond the "true" E2EE that policymakers have often implicitly assumed to be the only form. Notably, lawful access is possible in common scenarios where the government can access content that the device uploads to the cloud, as well as content sent or received through SaaS services. In assessing government arguments that they are "going dark," the prevalence of these other

137. See Ian Levy & Crispin Robinson, *Principles for a More Informed Exceptional Access Debate*, LAWFARE (Nov. 29, 2018), <https://www.lawfaremedia.org/article/principles-more-informed-exceptional-access-debate> [<https://perma.cc/MU79-DQWQ>].

138. See Susan Landau, *Exceptional Access: Devil Is in the Details*, LAWFARE (Dec. 26, 2018), <https://www.lawfaremedia.org/article/exceptional-access-devil-details-0> [<https://perma.cc/7P8P-5WEZ>].

139. Open Letter to GCHQ on the Ghost Proposal (May 22, 2019), https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf [<https://perma.cc/88E6-7K4Q>]; see Natasha Lomas, *Apple, Google, Microsoft, WhatsApp Sign Open Letter Condemning GCHQ Proposal to Listen in on Encrypted Chats*, TECHCRUNCH (May 30, 2019), <https://techcrunch.com/2019/05/30/apple-google-microsoft-whatsapp-sign-open-letter-condemning-gchq-proposal-to-listen-in-on-encrypted-chats/> [<https://perma.cc/48JH-N3WN>].

scenarios shows that lawful access today is often achievable despite the existence of E2EE messaging.

We next turn to major ways that E2EE is used today for purposes other than simply sending a message from Alice to Bob. For situations where policymakers are considering limits on E2EE, the analysis here shows large and perhaps unexpected possible consequences of blanket regulation. Along with the cogent arguments against outlawing E2EE for messaging, these other E2EE situations show important risks from laws limiting E2EE generally.

We summarize, for a legal and policy audience, three ways E2EE is pervasively used in current online computing: (1) Transport Layer Security (TLS); (2) Secure Shell (SSH); and (3) the class of Virtual Private Networks (VPNs), which use TLS and other protocols as well. These are three examples of E2EE—communication is protected between Alice and Bob, there is never a time when the unencrypted content would be available to a wiretap or man-in-the-middle attack. As a law and policy matter, any categorical legal limits on the use of E2EE would thus undermine protocols vital to the modern Internet, going far beyond messaging, with severe effects on cybersecurity.

1. Transport Layer Security.

One widespread use of TLS is to provide security for web traffic. TLS and HTTPS, the secure version of HTTP, enable web browsers (clients) to request, and servers to send, web pages, images, and videos. Since the Swire and Ahmad encryption articles were published in 2012, there has been explosive growth in the use of HTTPS, an expansion that accelerated after the 2013 Snowden disclosures described in Part III. After Snowden, Google began favoring HTTPS in its search rankings.¹⁴⁰ Let's Encrypt, a certificate authority launched in 2015, provided free certificates that removed the cost barrier to enabling encryption.¹⁴¹ Browser

140. Bill Budington, *Google Boosts Secure Sites in Search Results*, ELEC. FRONTIER FOUND. (Aug. 8, 2014), <https://www.eff.org/deeplinks/2014/08/google-boosts-secure-sites-search-results> [<https://perma.cc/7FTV-WC45>].

141. *Encryption for Everybody: A Non-Profit Providing Free TLS Certificates to More than 700M Websites*, LET'S ENCRYPT, <https://letsencrypt.org/> [<https://perma.cc/7C7R-92S6>] (last visited Mar. 10, 2026); see *New, Free Certificate Authority to Dramatically Increase Encrypted Internet Traffic*, ELEC. FRONTIER FOUND. (Nov. 18, 2014), <https://www>.

makers began displaying warnings on unencrypted sites.¹⁴² By 2024, more than ninety percent of web page loads used HTTPS.¹⁴³ E2EE between clients and servers thus became the norm—there were changes to the core protocols of the Internet, developed through international standards bodies and adopted by every major browser, server, and cloud platform.¹⁴⁴

In addition, E2EE via TLS secures many types of network traffic beyond just HTTPS web browsing. Because TLS is independent of the application layer, it acts as a secure wrapper for various protocols, including email (SMTP/IMAP/POP3), file transfers (FTPS), virtual private networks (VPNs), and database connections.¹⁴⁵ Standards have developed extensions to TLS that perform additional functions. For instance, even on encrypted connections, an observer previously could see which specific website a user was connecting to, even if the observer could not see what the user did on that site. Standards bodies have developed extensions that encrypt not only content, but also which services users connect to in the first place.¹⁴⁶

eff.org/press/releases/new-free-certificate-authority-dramatically-increase-encrypted-internet-traffic [https://perma.cc/3QCJ-D96Q].

142. Chester Wisniewski, *The State of World Wide Web Security in 2021*, SOPHOS (Nov. 22, 2021), <https://www.sophos.com/en-us/blog/the-state-of-world-wide-web-security-in-2021> [https://perma.cc/7SZG-WW56]; Jason Kelley, *EFF at 30: Surveillance Is Not Obligatory, with Edward Snowden*, ELEC. FRONTIER FOUND. (June 2, 2021), <https://www.eff.org/deeplinks/2021/05/eff-30-surveillance-isnt-prerequisite-edward-snowden> [https://perma.cc/4CCH-8V8K].

143. *HTTPS Encryption on the Web*, GOOGLE: TRANSPARENCY REP., <https://transparencyreport.google.com/https/overview?hl=en> [https://perma.cc/77E9-Y8NP] (last visited Mar. 10, 2026).

144. *What Is End-to-End Encryption: A Developer's Complete Guide*, DIGIT. TOOLPAD (Jan. 16, 2026), <https://www.digitaltoolpad.com/blog/what-is-end-to-end-encryption> [https://perma.cc/A9M9-RCBX]; Robert Dougherty, *Exploring E2EE: Real-World Examples of End-to-End Encryption*, KITEWORKS (June 30, 2025), <https://www.kiteworks.com/secure-file-sharing/real-world-examples-of-end-to-end-encryption/> [https://perma.cc/9S89-S47D]; TECH AGAINST TERRORISM, *TERRORIST USE OF E2EE: STATE OF PLAY, MISCONCEPTIONS, AND MITIGATION STRATEGIES 14* (2021), <https://www.techagainstterrorism.org/hubfs/TAT-Terrorist-use-of-E2EE-and-mitigation-strategies-report-.pdf> [https://perma.cc/JX8D-2PZU].

145. *Networking Secure Protocols*, MEDIUM (Feb. 10, 2025), <https://medium.com/@demegorash/networking-secure-protocols-725e6578013d> [https://perma.cc/49EM-287A]; *TLS Basics*, INTERNET SOC'Y, <https://www.internetsociety.org/deploy360/tls/basics/> [https://perma.cc/RX9X-5EVS] (last visited Mar. 10, 2026).

146. C. HUITEMA, INTERNET ENG'G TASK FORCE, *RFC 8744, ISSUES AND REQUIREMENTS FOR SERVER NAME IDENTIFICATION (SNI) ENCRYPTION IN TLS* (2020), <https://datatracker.ietf.org/doc/html/rfc8744> [https://perma.cc/Z866-B9DL].

2. Secure Shell.

Law and policy experts may have heard of SSH without having a clear sense of its importance. Cloudflare has defined the most common SSH use cases as: “[r]emotely managing servers, infrastructure, and employee computers; [s]ecurely transferring files (SSH is more secure than unencrypted protocols like FTP); [a]ccessing services in the cloud without exposing a local machine’s ports to the Internet; [c]onnecting remotely to services in a private network; and, [b]ypassing firewall restrictions.”¹⁴⁷ SSH is used ubiquitously in managing the world’s most sensitive computer systems.¹⁴⁸ SSH qualifies as E2EE in the same way messaging does, as when Alice remotely manages a server or employee computer used by Bob. A law limiting E2EE in general, and including the SSH protocol, would thus severely impact online security.¹⁴⁹

3. Virtual Private Networks.

A VPN is “an Internet security service that allows users to access the Internet as though they were connected to a private network. VPNs use encryption to create a secure connection over

147. *What Is SSH? Secure Shell (SSH) Protocol*, CLOUDFLARE, <https://www.cloudflare.com/learning/access-management/what-is-ssh/> [<https://perma.cc/Q7LM-ME62>] (last visited Mar. 10, 2026).

148. SSH Communications Security, the original developer of the SSH protocol, emphasizes the importance of SSH for high-impact users, claiming “.5% of users represent up to 99.5% of your cyber risk exposure.” *Secure Access for Systems, APIs, Workloads Without Keys or Passwords*, SSH, <https://www.ssh.com/products> [<https://perma.cc/URY2-HWAC>] (last visited Mar. 10, 2026).

149. For explanation of the importance of SSH to cybersecurity, *see, e.g.*, TATU YLONEN ET AL., NAT’L INST. OF STANDARDS & TECH., NISTIR 7966, SECURITY OF INTERACTIVE AND AUTOMATED ACCESS MANAGEMENT USING SECURE SHELL (SSH) (2015); T. YLONEN & C. LONVICK, INTERNET ENG’G TASK FORCE, RFC 4251, THE SECURE SHELL (SSH) PROTOCOL ARCHITECTURE (2006), <https://datatracker.ietf.org/doc/html/rfc4251> [<https://perma.cc/7LHM-FXRP>]; T. YLONEN & C. LONVICK, INTERNET ENG’G TASK FORCE, RFC 4252, THE SECURE SHELL (SSH) AUTHENTICATION PROTOCOL (2006), <https://datatracker.ietf.org/doc/html/rfc4252> [<https://perma.cc/9H7J-PZ4R>]; T. YLONEN & C. LONVICK, INTERNET ENG’G TASK FORCE, RFC 4253, THE SECURE SHELL (SSH) TRANSPORT LAYER PROTOCOL (2006), <https://datatracker.ietf.org/doc/html/rfc4253> [<https://perma.cc/Y7XK-NDZ2>]; T. YLONEN & C. LONVICK, INTERNET ENG’G TASK FORCE, RFC 4254, THE SECURE SHELL (SSH) CONNECTION PROTOCOL (2006), <https://datatracker.ietf.org/doc/html/rfc4254> [<https://perma.cc/KD8Y-C8NX>].

unsecured Internet infrastructure.”¹⁵⁰ Personal VPNs “encrypt internet traffic, mask IP addresses, and protect internet users on public Wi-Fi.”¹⁵¹ Enterprise VPNs also “offer centralized management, role-based access control, and dedicated infrastructure.”¹⁵² Both types of VPNs block wiretaps and prevent man-in-the-middle attacks, including by government agencies. Although some VPNs use TLS or SSH, VPNs constitute a broader class of software that can use other protocols including IPsec, L2TP, OpenVPN, and WireGuard.¹⁵³ A law or policy restricting VPNs thus would create significant security risks.

D. E2EE Beyond Confidentiality: Integrity, Authentication, and Authenticity

The preceding discussion in Part IV has addressed how E2EE can preserve *confidentiality*, defined as the “[p]roperty that information is not made available or disclosed to unauthorised individuals, entities, or processes.”¹⁵⁴ Sub-part IV.B discussed the five scenarios relevant to determining when confidentiality exists in E2EE messaging. Sub-part IV.C showed how confidentiality is preserved at other layers of the technology stack, such as TLS for web traffic and SSH for creating an encrypted channel for communication over an insecure network such as the Internet.

Confidentiality is the “C” in the widely known “CIA Triad” for cybersecurity:¹⁵⁵ “confidentiality, integrity, and availability.” E2EE is not predominantly deployed to ensure *availability*, defined as the “[p]roperty of being accessible and useable upon demand by an

150. *VPN Security: How VPNs Help Secure Data and Access Control*, CLOUDFLARE, <https://www.cloudflare.com/learning/access-management/vpn-security/> [https://perma.cc/KN9S-RV2L] (last visited Mar. 10, 2026).

151. *What Is a VPN? A Complete Guide to Virtual Private Networks*, PALO ALTO NETWORKS, <https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn> [https://perma.cc/BZ8W-W7PS] (last visited Mar. 10, 2026).

152. *Id.*

153. *Types of VPNs and Protocols*, NORDLAYER, <https://nordlayer.com/learn/vpn/types-and-protocols/> [https://perma.cc/QZ6A-7NLK] (last visited Mar. 14, 2026).

154. *Glossary: Confidentiality*, WORLD ECON. F., <https://widgets.weforum.org/blockchain-toolkit/glossary/index.html> [https://perma.cc/3A3J-EXQV] (last visited Mar. 10, 2026).

155. *CIA Triad*, FORTINET, <https://www.fortinet.com/resources/cyberglossary/cia-triad> [https://perma.cc/MD2N-NZM4] (last visited Mar. 10, 2026).

authorised entity.”¹⁵⁶ Encryption can reduce *availability* because it may “introduce latency, increase processing demands, or cause accessibility issues during outages.”¹⁵⁷

By contrast, as discussed in this Sub-part, encryption has become enormously important for data *integrity*, “the property that the data used in a solution is correct, reliable, and useful for all participants.”¹⁵⁸ The term applies “not only to a resistance to unintended data modification, but also to the completeness, timeliness, and accuracy of the data over its entire lifetime.”¹⁵⁹

Encryption is also now deeply intertwined with *authentication* and the closely related concept of *authenticity*. Authentication focuses on the “who”—“[v]erifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.”¹⁶⁰ Authenticity more broadly provides “assurance that data, communications, and identities are genuine, verified, and trustworthy.”¹⁶¹

As discussed here, beyond protecting confidentiality, E2EE is deployed at many layers of the technology stack to ensure data *integrity*, *authentication*, and *authenticity*. Any legal measures limiting E2EE thus risk disrupting multiple vital aspects of modern computing.

1. Data integrity, blockchain, and digital signatures

This Article has not yet focused on how blockchain, or other advanced cryptographic constructions, may be impacted by cryptography regulation. We now briefly discuss the role that

156. *Glossary: Availability*, WORLD ECON. F., <https://widgets.weforum.org/blockchain-toolkit/glossary/index.html> [<https://perma.cc/3A3J-EXQV>] (last visited Mar. 10, 2026).

157. Andrew Dennis, *CIA Triad: Definition, Importance, and Examples*, LUMOS, <https://www.lumos.com/topic/cia-triad> [<https://perma.cc/3TC9-S5FV>] (last visited Mar. 10, 2026).

158. *Glossary: Integrity*, WORLD ECON. F., <https://widgets.weforum.org/blockchain-toolkit/data-integrity/index.html> [<https://perma.cc/3A3J-EXQV>] (last visited Mar. 10, 2026).

159. *Id.*

160. *Glossary: Authentication*, WORLD ECON. F., <https://widgets.weforum.org/blockchain-toolkit/glossary/index.html> [<https://perma.cc/3A3J-EXQV>] (last visited Mar. 10, 2026) (citing NAT’L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-63-3, DIGITAL IDENTITY GUIDELINES (2017)).

161. *Authenticity*, ARTOON SOLUTIONS, <https://artoonsolutions.com/glossary/authenticity/> [<https://perma.cc/6EHF-MKXQ>] (last visited Mar. 14, 2026).

blockchains, built on encryption, play in promoting data integrity. In its detailed study on data integrity, the World Economic Forum stated:

Once data is entered and confirmed through the consensus process, blockchain technology provides strong protection from further changes, since those changes would be easily noticed by other participants on the network. Thus, blockchain helps to establish a higher level of traceability and auditability to data so that any data that was entered inaccurately prior to consensus can be traced back to its origin.¹⁶²

Thus, by providing “strong protection from further changes,” a well-implemented blockchain system can support data integrity. Most famously, such systems have been applied for cryptocurrency transactions, where value is transferred without using a third-party intermediary such as a bank and transactions are decentralized—roughly, not controlled by a government or central bank.¹⁶³ Our research has not found instances where proposed regulation of E2EE generally was designed to regulate cryptocurrencies or blockchain systems. However, measures that compromise key material could still affect crypto users, whose wallets depend entirely on key security. Given the growing scale of blockchain and cryptocurrency adoption, maintaining data integrity, through E2EE, matters here too.

2. Zero-Trust Architecture and Authentication in Encryption

Policymakers have embraced encryption that includes authentication by widespread support for “Zero Trust Architecture” (ZTA). Previously, many organizations secured their systems using a perimeter-based approach—building a strong boundary around the network and trusting everything inside it.¹⁶⁴

162. *Data Integrity*, WORLD ECON. F., <https://widgets.weforum.org/blockchain-toolkit/data-integrity/index.html#solutions-for-data-integrity-in-a-blockchain-context> [<https://perma.cc/DQ9S-QZFM>] (last visited Feb. 4, 2026).

163. Nathan Peterson, *What Is Cryptocurrency and How Does It Work?*, CHARLES SCHWAB (May 6, 2025), <https://www.schwab.com/learn/story/cryptocurrencies-what-are-they> [<https://perma.cc/2M76-FWL2>].

164. “Many legacy architectures rely on perimeter-based security models such as TIC 2.0 that routes all traffic through centralized controls.” Press Release, Cybersecurity & Infrastructure Sec. Agency, New CISA Guide Assists Federal Agencies with Transitioning to Modernized Zero Trust Architectures (June 24, 2026), <https://www.cisa.gov/news->

Under the perimeter-based approach, encryption was applied to data entering or leaving the network; internally, systems communicated freely without encryption while externally, encryption was applied only at the network perimeter. Ongoing data breaches demonstrated the weakness of the perimeter-based approach—once an attacker penetrated the perimeter, such as through a phishing email, a compromised vendor, or a stolen credential, they could move freely through internal systems precisely because those systems trusted each other by default.

In response, ZTA has been adopted broadly and is often legally mandated. The core principle is that no connection should be trusted simply because of where it originates. Every communication between users, devices, and services must be encrypted and authenticated, whether it crosses the open Internet or travels between two servers in the same building.¹⁶⁵

US policy has adopted ZTA, with its encryption and authentication components. Executive Order 14028, issued in 2021, directs federal agencies to adopt Zero Trust models.¹⁶⁶ Encryption is not merely a feature within these systems but the structural assumption on which the entire security model depends. An Office of Management and Budget memorandum, to implement the Executive Order, requires agencies to encrypt all network traffic “as soon as practicable” and to treat every application as Internet accessible.¹⁶⁷ The Department of Defense Zero Trust Reference Architecture states the point without qualification: “[e]ncryption is a key part of the ZT Architecture. Without, encryption files are left in plain text which can expose sensitive information.”¹⁶⁸ The European Union is similarly moving forward with ZTA implementation, such as through its Network and

events/news/new-cisa-guide-assists-federal-agencies-transitioning-modernized-zero-trust-architectures [https://perma.cc/RZP4-C26E].

165. SCOTT ROSE ET AL., NAT’L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-207, ZERO TRUST ARCHITECTURE (2020).

166. Improving the Nation’s Cybersecurity, Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021).

167. Memorandum from Shalanda D. Young, Acting Dir., Off. of Mgmt. & Budget, to Heads of Exec. Dep’ts & Agencies, M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (Jan. 26, 2022).

168. U.S. DEP’T OF DEF., ZERO TRUST REFERENCE ARCHITECTURE (version 2.0, 2022) (prepared by the Defense Information Systems Agency & National Security Agency Zero Trust Engineering Team).

Information Systems Directive 2,¹⁶⁹ applying to critical infrastructure, and the Digital Operational Resilience Act, applying to the financial sector.¹⁷⁰

ZTA relies extensively on E2EE to provide encryption and authentication for communications between each node of even internal networks. Any legal limit on the use of E2EE for ZTA would be enormously disruptive. Such a requirement would mean redesigning these systems around a fundamentally different premise, one that reintroduces the very assumption of implicit trust that Zero Trust was developed to eliminate. The federal government has invested years and considerable resources in moving away from perimeter-based approaches, because that model was inadequate.¹⁷¹ Mandating government access between nodes would reverse that direction, contrary to the cybersecurity principles adopted after the failure of systems without ZTA. Critically, US and EU law already require use of E2EE through ZTA, meaning restrictions on E2EE would conflict with their own policies.¹⁷²

V. *CONCLUSION: POLICY LESSONS FOR ROUND 3 OF THE GOING DARK DEBATE*

As articulated in this Article, Round 3 of the Going Dark Debate concerns E2EE. Those seeking to set limits on E2EE might initially seem to have a stronger case than they did for Rounds 1 and 2. At the end of the Crypto Wars in Round 1, the United States lifted nearly all export controls, making strong encryption lawfully

169. Cristina-Ioana Călin & Andreea-Mihaela Comșîț, *A Comprehensive Review of Cybersecurity for Modern Work: Attacks, Zero Trust and NIS2 Compliance*, 13 J. COMPUT. & COMM'NS 138 (2025); see *NIS2 Directive: Securing Network and Information Systems*, EUR. COMM'N, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> [<https://perma.cc/AJR5-23PX>] (last visited Mar. 10, 2026).

170. *Zero Trust Guidance for Achieving Operational Resilience*, CLOUD SEC. ALLIANCE (Apr. 6, 2026), <https://cloudsecurityalliance.org/artifacts/zero-trust-guidance-for-achieving-operational-resilience> [<https://perma.cc/L3X3-KXPY>]; see *Digital Operational Resilience Act (DORA)*, EUR. INS. & OCCUPATIONAL PENSIONS AUTH. (Dec. 15, 2025), https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [<https://perma.cc/J7RC-DYGY>].

171. See Peterson, *supra* note 163; see also Riccardo Di Blasio, *The Perimeter Is Gone. Security Has to Follow the Data*, NEXTGOV/FCW (July 29, 2026), <https://www.nextgov.com/ideas/2026/07/perimeter-gone-security-has-follow-data/415100/> [<https://perma.cc/9RH4-TMMZ>].

172. See *CIA Triad*, *supra* note 155; *Glossary: Integrity*, *supra* note 158.

available for international communications and commerce. Law enforcement and national security agencies, however, could often succeed in gaining lawful access to content, notably because strong encryption was not used widely enough to block many actual investigations. For Round 2 of the Going Dark Debate, our discussion showed that encryption in transit was becoming widespread; fortunately for lawful access, emails and the plaintext of a vast array of other content were available in stored records, often held in the cloud. For Round 3, however, Alice can readily use E2EE to communicate with Bob. In the “true” or “implicitly assumed” E2EE shown in our Scenario 1, no entity between Alice and Bob can read the plaintext. For law enforcement and national security agencies, and their allies such as those combating CSAM, Round 3 is categorically different—at no point in the communication from Alice to Bob can lawful access reach the plaintext.

A. Surprisingly Often, Lawful Access Can Gain Access to Messages

It is important both to recognize the logic of this *prima facie* case, and to appreciate the many reasons this Article has identified for skepticism about laws that prohibit E2EE. For supporters of lawful access to E2EE content, the intuition is that “we lack the technology to read the communication from Alice to Bob,” and so we should pass laws to change the technology. Our discussion of the scenarios, however, showed the enormous gap between the premise that law enforcement cannot break E2EE as a technical matter and the conclusion that law enforcement cannot in fact gain access to the encrypted content. The first is true; the second, as Scenarios 2 through 4 demonstrate, frequently is not.

For Scenario 1, with “true” E2EE, the facts don’t support the claim that ordinary users are predominantly adopting E2EE. The estimated 2 billion TikTok users do not have E2EE for messaging, nor would other services based in China, where use of E2EE for messaging is prohibited.¹⁷³ Instagram’s 2026 decision to stop supporting E2EE illustrates that platforms and services may have business or policy reasons not to offer E2EE.¹⁷⁴ In addition, law

173. See Tidy, *supra* notes 91.

174. See Lakshmanan, *supra* note 90.

enforcement may gain access to a user's device and use methods such as a fingerprint to gain access to the content.¹⁷⁵

Scenario 2 exists when government can access content backed up to the cloud. Many users face the risk of losing important content if their phone or other device is lost or stops working. Both Android and iOS users have the option to have encrypted backup, where only the user holds the keys. Available evidence suggests that most users have not enabled such backup features.¹⁷⁶ There are cybersecurity risks for users who keep their own keys. If those keys are lost, there is no way to recover the content. Adoption of strongly encrypted backup—with content unavailable even to Apple or Google—thus may remain possible but far from dominant.

Scenario 3 exists where the government can gain access through SaaS. That is, even when the “endpoint” of E2EE is controlled by Bob, Bob's software service would open the communication, and the software service would be subject to lawful access. As documented above, a wide range of SaaS are now in common use, including for Microsoft 365 (including Microsoft Teams) and Google Workspace (including Gmail and Google Docs).

Scenario 4 exists where lawful access is possible due to software on Bob's device. Such software may exist as part of the device's operating system or other software, such as the Apple CSAM proposal that the company eventually withdrew. Governments from various countries have used Pegasus and other

175. Ethan Swierczewski, *Passcodes, Protection, and Legal Practicality: The Necessity of a Digital Fifth Amendment*, 31 CATH. U. J.L. & TECH. 189 (2022); Aaron Chase, *Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments*, 17 HASTINGS RACE & POVERTY L.J. 604 (2020); MICHAEL A. FOSTER, CONG. RSCH. SERV., LSB10416, CATCH ME IF YOU SCAN: CONSTITUTIONALITY OF COMPELLED DECRYPTION DIVIDES THE COURTS (2020); Harrison Metz, “Your Device Is Disabled”: How and Why Compulsion of Biometrics to Unlock Devices Should Be Protected by the Fifth Amendment Privilege, 53 VAL. U. L. REV. 427 (2019).

176. See *50+ Cloud Security Statistics in 2026*, SENTINELONE (Feb. 16, 2026), <https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/> [<https://perma.cc/T65N-Y4EJ>] (“Over 21% of organizations worldwide have encrypted over 60% of their classified data on the cloud.”); *Personal Cloud Storage Use: How Many People Use the Cloud? (2025)*, THREADGOLD CONSULTING (Feb. 2, 2025), <https://threadgoldconsulting.com/research/personal-cloud-storage-usage> [<https://perma.cc/DEE6-YJNY>] (“A 2024 UK survey found that 43% of users were concerned about their cloud provider scanning personal data. As a result, encrypted storage and zero-knowledge platforms are growing in popularity.”).

spyware to gain access to content in this way.¹⁷⁷ There have been intense debates about whether and under what restrictions software that enables governments to gain remote access to devices should be permitted by law.¹⁷⁸ The possibility of such access, however, exists if governments can place software onto a user's device. Scenario 4 shows that on-device software offers a path to lawful access that does not require breaking E2EE at the network level.

B. E2EE Is Used for Multiple, Vital Layers of the Technology Stack

Beyond messaging, E2EE is used in multiple and essential ways for different parts of modern computing. We have explained vital ways that E2EE is used to protect confidentiality, including for web traffic through TLS and HTTPS and secure communications using SSH. We have also explained that E2EE is used for goals beyond *confidentiality*, notably for data *integrity*, *authentication*, and *authenticity*. For data integrity, we highlighted the importance of blockchain. Perhaps most importantly, authenticated E2EE is a required element for Zero Trust Architecture, often required under US and EU law.

This list of vital E2EE software is far from complete. The Internet Engineering Task Force (IETF) has maintained since 2000 that Internet protocols should not include built-in surveillance

177. Emma Vitale, *Spyware in the Wrong Hands: What Can Governments Do?*, AM. U. (July 18, 2025), <https://www.american.edu/sis/news/20250718-spyware-in-the-wrong-hands-what-can-governments-do.cfm> [<https://perma.cc/Q3EW-CKLS>].

178. Bellovin et al., *Going Bright*, *supra* note 114; see Bellovin et al., *Lawful Hacking*, *supra* note 79; see also O.L. van Daalen, *The Right to Encryption: Privacy as Preventing Unlawful Access*, 49 COMPUT. L. & SEC. REV. 105804 (2023); Pragya Jain, *Encryption: A Tradeoff Between User Privacy and National Security*, AM. U. (July 15, 2021), <https://www.american.edu/sis/centers/security-technology/encryption.cfm> [<https://perma.cc/XG6C-449Q>].

mechanisms,¹⁷⁹ a principle the IETF has reaffirmed over time.¹⁸⁰ National Institute of Standards and Technology (NIST) Special Publication 800-53, the federal government's primary catalog of security and privacy controls, requires cryptographic protection for data in transit and at rest across all system impact levels.¹⁸¹ These controls assume the availability of strong, uncompromised encryption as a baseline.

We draw attention to these multiple, vital uses of E2EE in part because our research has not found similar previous discussions. It is too easy for a government agency or supporter of CSAM legislation to argue that E2EE is dangerous and the law should limit it. The discussion here shows, instead, that E2EE is pervasively deployed in numerous and vital parts of the technology stack. In addition, the IETF has maintained for many years that E2EE should be the *default* architecture—Internet protocols should not include built-in surveillance mechanisms.

In conclusion, on the extensive use of E2EE across the technology stack, policy debates should recognize that E2EE is the norm for numerous aspects of modern computing. The arguments

179. The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards. . . . The IETF, an international standards body, believes itself to be the wrong forum for designing protocol or equipment features that address needs arising from the laws of individual countries, because these laws vary widely across the areas that IETF standards are deployed in. Bodies whose scope of authority correspond to a single regime of jurisdiction are more appropriate for this task.

IAB & IESG, INTERNET ENG'G TASK FORCE, RFC 2804, IETF POLICY ON WIRETAPPING (2000), <https://www.rfc-editor.org/info/rfc2804> [<https://perma.cc/EFS7-89P6>].

180. This document describes practices currently used by network operators to manage, operate, and secure their networks and how those practices may be impacted by a shift to increased use of encryption. . . . This document does not endorse the use of the practices described herein, nor does it aim to provide a comprehensive treatment of the effects of current practices, some of which have been considered controversial from a technical or business perspectives or contradictory to previous IETF statements . . . The following RFCs consider the end-to-end (e2e) architectural principle to be a guiding principle for the development of Internet protocols . . . This document aims to help IETF participants understand network operators' perspectives about the impact of pervasive encryption, both opportunistic and strong end-to-end encryption, on operational practices.

K. MORIARTY & A. MORTON, INTERNET ENG'G TASK FORCE, RFC 8404, EFFECTS OF PERVASIVE ENCRYPTION ON OPERATORS (2018), <https://www.rfc-editor.org/rfc/rfc8404> [<https://perma.cc/ZAB9-9RTD>].

181. NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-53, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (rev. 5 2020).

against backdoors—against building surveillance into software—have won in domain after domain. For ZTA and elsewhere, the law affirmatively requires the use of E2EE. Any general ban on E2EE would therefore create enormous cybersecurity problems throughout modern computing.

C. Unintended Cybersecurity and Other Consequences of Legal Limits on E2EE

As a matter of legal definition, the pervasive use of E2EE across the technology stack makes it enormously challenging to meet the goals of lawful access (access the content of communications) without undermining the cybersecurity of essential software protocols.

Take a law focused on messaging, which seeks to require technical access for messages sent from Alice to Bob. First, consider a narrow definition, perhaps focused on named messaging services that use E2EE such as iMessage, Signal, and WhatsApp. With this law, notice how readily messages can be sent through one of the other E2EE mechanisms. For instance, any web page can communicate securely with Bob using TLS. Any node can similarly use SSH to send a secure communication to Bob. Even if such services are not common today, they may easily grow if a law degrades the usefulness of traditional messaging apps. In short, the category of software that sends confidential messages is much, much broader than the named messaging services.

Second, consider a broader definition, which would require limits on E2EE for confidential transmission of content from Alice to Bob. As discussed in the overall Conclusion below, the wide reach of E2EE means any overbroad regulation would undermine the cybersecurity of numerous aspects of modern computing.

As a matter of law and policy, it is a serious problem that there is no clear boundary between E2EE for communication that we wish to regulate and E2EE for communication that we do not wish to regulate. This Article has discussed the actuality and desirability of using E2EE across the technology stack. Any proposal to limit E2EE for messaging must face the lack of meaningful technical distinction between the software that law enforcement has targeted and other essential software that similarly uses E2EE.

D. Overall Conclusion: The Continued Persuasiveness of “Least Trusted Country” and “Golden Age of Surveillance”

This Article has focused on lawful access to content, primarily for law enforcement and national security purposes. As in Rounds 1 and 2 of the Going Dark Debates, government agencies have understandably been concerned about losing access to evidence that they might have previously accessed. In Round 3, such agencies face E2EE, where no entity between Alice and Bob can read the plaintext. Confronted with this increasingly common technical reality, government agencies and others have sought laws to create some technical mechanism to access that content.

The fact that certain communications are no longer available for lawful access as a technical matter does not mean there is any better legal alternative. Based on review of developments since the 2012 article by Swire and Ahmad, key arguments from Round 2 are highly persuasive once again in Round 3.

The “least trusted country” argument applies at least as much today as it did in 2012. The argument stresses that encryption broken for the benefit of one country would also be broken for the benefit of other countries, including those one trusts the least. That is, a backdoor accessible remotely by one country is also technically available to all other countries. Here is where dramatic harm can come from an overbroad law regulating E2EE—consider the risk from a backdoor for the many protocols that use E2EE, such as TLS and SSH. The harm would spread beyond the stated purpose of providing lawful access to E2EE messages, reaching numerous other parts of the technology stack covered by the overbroad regulation.

Next, consider the empirical limits on government claims that they are “going dark.” A surprisingly large fraction of messaging does not match the “true” or “implicitly assumed” version of E2EE in Scenario 1. In practice, the government often retains lawful access through cloud backup, SaaS, or on-device software (Scenarios 2, 3, and 4). This empirical reality on messaging is markedly different from any government claims that it is “going dark,” and that modern technology broadly blocks investigations.

Just as the “darkness” is less severe than portrayed, the “golden age of surveillance” has continued, and provides government access to unprecedented information about

individuals. The 2012 article catalogued how government surveillance at that time was far easier than in earlier periods. Compared to 2012, government agencies today have powerful additional investigatory tools. Facial recognition is far more precise than previously, and cameras are ubiquitous in public places.¹⁸² Drones and the myriad devices of the Internet of Things gather data in unprecedented ways.¹⁸³ Data brokers have expanded their offerings, based in part on the enormous volume of social media posts.¹⁸⁴ Perhaps most importantly, all of this unprecedented data is processed by artificial intelligence, which can help investigators spot patterns that were previously undetected.¹⁸⁵ Indeed, Harvard Professor Shoshana Zuboff has argued that we are living in “The Age of Surveillance Capitalism.”¹⁸⁶

In sum, the case remains in Round 3 of the Going Dark Debate that government is not “going dark,” and that proposed limits on encryption would harm cybersecurity, privacy, and the effectiveness of commerce and government agencies. E2EE is deployed throughout the technology stack. It is a feature of modern computing, and not a bug to eliminate or restrict.

182. Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/> [https://perma.cc/YHV8-KW5A]; JULIAN SLAUGHT & RYAN LECLOUX, WIS. LEGIS. REFERENCE BUREAU, FACIAL RECOGNITION TECHNOLOGY: BALANCING SAFETY AND PRIVACY (2020); see Jake Parker & David Ray, *What Science Really Says About Facial Recognition Accuracy and Bias Concerns*, SEC. INDUS. ASS'N (July 23, 2022), <https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/> [https://perma.cc/EA56-VVQH].

183. Anita Choudhary, *Internet of Things: A Comprehensive Overview, Architectures, Applications, Simulation Tools, Challenges, and Future Directions*, 4 DISCOVER INTERNET OF THINGS 31 (2024); Asif Mahmud Raivi & Sangman Moh, *A Comprehensive Survey of Data Aggregation Techniques in UAV-Enabled Internet of Things*, 50 COMPUT. SCI. REV. 100599 (2023).

184. See Tom Kemp, *How Data Brokers Profile, Segment, and Score Us*, MEDIUM (July 26, 2023), <https://tomkemp00.medium.com/how-data-brokers-profile-segment-and-score-us-5144af9a465> [https://perma.cc/R2SX-FZRH].

185. *AI-Driven Analysis in Digital Forensics: Uncovering Patterns from Pixels*, EFORENSICS MAG. (Aug. 29, 2023), <https://eforensicsmag.com/ai-driven-analysis-in-digital-forensics-uncovering-patterns-from-pixels/> [https://perma.cc/F4Y2-DY6L].

186. SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (2019).