After Stockholm: Can Cyber Diplomacy Reconcile Lawful Access and Strong Encryption?

A UK–Sweden symposium brings cross-border digital evidence back into focus. The central challenge is to improve legitimate investigations while preserving strong encryption, effective oversight and public trust.

Vladimir Tsakanyan, Ph.D. · Center for Cyber Diplomacy and International Security

November 28, 2026

Cover image: AI-generated conceptual illustration; it does not depict an actual meeting or facility.

A criminal investigation crosses a border long before a detective does. A message may be sent from one country, stored by a company in another and connected to a suspect or victim in a third. Authorities seeking evidence must navigate different legal standards, different providers and, increasingly, technical designs that prevent the provider from reading the content at all.

A meeting in Stockholm put those tensions on the diplomatic agenda. On November 27, 2026, the United Kingdom published the co-chairs' readout of the second International Symposium on Lawful Access, held on November 17–18 and co-chaired by the UK and Sweden. Participants included representatives from 36 countries and international organisations, alongside people from the technology sector, civil society and academia. The readout describes discussion and cooperation; it does not announce a treaty, a new surveillance law or an agreed technical mechanism. [1]

The policy challenge is often framed as a choice between public safety and privacy. That framing is too narrow. Strong encryption is itself a public-safety tool, protecting hospitals, infrastructure, businesses, journalists and ordinary communications. At the same time, serious crimes produce real investigative needs. A durable international approach must ask four separate questions: what officials may lawfully seek, what information actually exists, who can access it, and which jurisdiction and safeguards apply.

What Stockholm did—and did not—decide

According to the co-chairs, the symposium considered cross-border access to data, international cooperation, emerging technologies and the future operating environment for law enforcement and security agencies. Participants exchanged national experiences and

discussed rights-respecting approaches. The Home Office describes this as a forum for dialogue; the brief public readout does not identify a single technical standard, bind participants to legislation or disclose a detailed negotiating text. [1]

Those limits are important. A diplomatic statement about cooperation should not be read as proof that governments have agreed to require a backdoor in encrypted services. Nor does it resolve the disagreements between investigators, technology providers and civil society. Its significance is institutional: governments are continuing to coordinate around a problem that no national police service can solve on its own.

For investigators dealing with child exploitation, organized crime, terrorism or ransomware, delay can have consequences. Evidence may disappear, a victim may remain at risk or suspects may move between jurisdictions. Agencies therefore argue for workable processes through which service providers can preserve and disclose data when an appropriate legal order exists. The co-chairs explicitly frame access as relevant to investigation and public protection while also referring to privacy and the rule of law. [1]

One request can involve several kinds of data

The phrase “access to data” can mean a range of different things. Subscriber information may identify an account holder. Connection records may describe when and from where a service was used. Stored files, messages or device backups may contain content. A provider may retain one category but not another, and different legal thresholds and retention periods can apply.

End-to-end encryption adds a further distinction. In a properly designed system, message content is encrypted so that only endpoints with the relevant keys can read it. A provider may be able to supply information in its possession while lacking a usable copy of the message content or the key needed to decrypt it. Whether a particular service works this way depends on its actual design, including devices, backups, account recovery and metadata practices.

That distinction matters for policy. An order that speeds delivery of existing subscriber records is not technically the same as a mandate to redesign encrypted messaging. A targeted forensic examination of a seized device is also different from building a general-purpose mechanism into every user’s communications. Each raises its own questions about legality, accuracy, collateral exposure and oversight.

The cross-border problem already has legal machinery

The United States and the United Kingdom provide one example of an existing arrangement. Their agreement on access to electronic data for serious-crime investigations entered into force on October 3, 2022. The U.S. Department of Justice says it enables providers in one country to respond to qualifying orders from the other, subject to specified conditions and

limitations. It is a bilateral framework operating within defined rules, not a general permission for either government to obtain anyone’s messages. [2]

For instance, the Justice Department says orders submitted by UK authorities under the agreement must not target U.S. persons or people located in the United States; U.S. orders under it must not target people located in the UK. Both sides must also meet the agreement’s other requirements. The usefulness of such arrangements depends not only on speed but on whether limits are checked, providers can identify valid requests, and errors can be challenged. [2]

The European Union’s electronic-evidence regulation offers a different model. Regulation (EU) 2023/1543 provides for European Production and Preservation Orders in criminal proceedings and applies from August 18, 2026, according to the EU’s legal summary. It concerns specified electronic evidence held by service providers and operates within its own scope and safeguards. The regulation’s text also states that its application should not affect the use of encryption by providers or users. [3] [4]

These frameworks address some problems of jurisdiction and process. They do not make inaccessible data readable by themselves. An efficient legal channel cannot compel a provider to produce a key it does not possess; conversely, faster requests do not remove the need to test the legality and proportionality of what is sought. Treating legal process and system design as separate questions makes the remaining disagreement more precise.

Europe’s roadmap is a policy agenda, not an enacted encryption solution

In June 2025, the European Commission presented a roadmap for effective and lawful access to data. It described work on data retention, interception, digital forensics, decryption, standardisation and the use of AI in processing evidence. The Commission said it intended to assess technologies for access to encrypted data while safeguarding cybersecurity and fundamental rights. These are policy directions and planned work; the 2025 announcement is not evidence that an encryption-breaking mandate has been enacted. [5]

The Commission also states that strong encryption is necessary for cybersecurity, data protection and privacy. Its published position is that measures addressing investigations must safeguard encryption. Whether future proposals meet that objective requires independent assessment of their precise design and implementation, rather than assuming that a general commitment settles the technical question. [6]

Policymakers should be equally cautious about treating future technology as an answer on its own. A research programme can evaluate possible approaches; it cannot guarantee that a method will work, scale safely or remain compatible with rights. Before any proposal is adopted, its proponents should identify which data is sought, which systems are affected,

who could exercise access and how the mechanism would be tested against misuse.

The security case for encryption

Encryption protects far more than private conversations. Banks use it to secure transactions; health services use it to protect sensitive records; governments rely on it for their own communications. Weaknesses introduced to facilitate access could become attractive targets for criminals or hostile intelligence services, particularly if access credentials or management systems are concentrated in one place.

In the 2015 research report “Keys Under Doormats,” computer scientists and security experts argued that broad exceptional-access requirements could introduce technical complexity and security vulnerabilities. Their analysis remains an important warning about systemic design choices, although it does not prove that every conceivable investigative tool has the same architecture or risk. Each proposed mechanism needs its own public threat model and independent review. [7]

A narrow legal warrant and a narrow technical capability are not automatically the same thing. A warrant may authorize access to one target, while a system built to facilitate repeated access could create a capability that others attempt to misuse. The reverse is also true: a privacy-preserving service can be designed and governed in different ways. Evaluating the actual mechanism is more useful than assuming that a label—whether “lawful access” or “backdoor”—settles every question.

Rights are practical design requirements

The European Court of Human Rights’ 2024 judgment in Podchasov v. Russia illustrates why safeguards and scope matter. The Court examined a Russian regime combining extensive retention, authorities’ access to communications and a decryption obligation, and found a violation of Article 8. Its assessment concerned that particular legal framework and its safeguards; it should not be simplified into a ruling on every possible form of digital investigation. [8]

For democratic governments, necessity and proportionality should be visible throughout the process. Who can authorize a request? Is there independent approval before access, and a meaningful record afterward? Can a provider contest an overbroad demand? Are affected individuals notified when doing so no longer jeopardizes an investigation? How are errors corrected and remedies provided? The answer may differ across systems, but these are operational requirements, not decorative language.

Cross-border requests add another layer. The government issuing an order, the provider receiving it and the person affected may be subject to different rules. Agreements need clear limits on purpose, onward sharing and retention; independent oversight; and procedures for resolving conflicts between legal obligations. A transparent aggregate report

can help the public evaluate a system without exposing a particular investigation.

A practical agenda for cyber diplomacy

First, governments should improve the speed and quality of requests for data that providers already hold. Standardized formats, trained personnel, secure channels and clear points of contact can reduce delay without requiring a change to cryptographic design. Measuring response times and rejected requests would help distinguish procedural bottlenecks from genuine technical limits.

Second, investigators should invest in lawful, targeted alternatives and examine their own risks. Depending on the case, relevant evidence may exist in a device lawfully obtained, in records a provider can access, through a cooperating participant, or in financial and physical evidence. None is a universal substitute for message content, and each requires appropriate authorization and protection against misuse.

Third, proposed technical access mechanisms should face independent security review before deployment. That review should include how credentials are protected, how abuse is detected, whether vulnerabilities could affect people outside the investigation, and whether the mechanism can be withdrawn if risks prove unacceptable. Researchers and affected communities need enough information to challenge assumptions, while sensitive operational details can remain protected.

Finally, cooperation should include civil society and technical specialists as participants rather than treating them as audiences for a finished plan. International agreement is more durable when the people responsible for security, legal oversight and the protection of vulnerable users can test proposals early. As the Stockholm readout itself acknowledges, the conversation spans government, industry, academia and civil society. [1]

The test after Stockholm

The November meeting did not settle the encryption debate. Its real value will be determined by what follows: whether governments can improve legitimate investigations while demonstrating that new measures are necessary, reviewable and technically defensible. International cooperation should make lawful requests more reliable and accountable, not merely move the same unresolved risks across borders.

Public safety and secure communications depend on institutions people can trust. The next phase of cyber diplomacy should therefore begin with the precise request, the available evidence and the actual system design. Only then can policymakers compare the investigative benefit of a proposal with its security costs and the rights it may affect.

Sources and links

[1] UK Home Office, International Symposium on Lawful Access 2026: co-chairs' readout, published November 27, 2026

https://www.gov.uk/government/publications/international-symposium-on-lawful-access-2026/international-symposium-on-lawful-access-2026-co-chairs-readout

[2] U.S. Department of Justice, U.S.–UK Data Access Agreement Enters into Force, October 3, 2022

https://www.justice.gov/archives/opa/pr/landmark-us-uk-data-access-agreement-enters-force

[3] EUR-Lex, Electronic evidence in criminal proceedings: production and preservation orders

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4649186

[4] Regulation (EU) 2023/1543 on European Production and Preservation Orders

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1543

[5] European Commission, Roadmap for effective and lawful access to data for law enforcement, June 24, 2025

https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en

[6] European Commission, Encryption and lawful access to data

https://home-affairs.ec.europa.eu/policies/internal-security/lawful-access-data/encryption_en

[7] Abelson and others, Keys Under Doormats, MIT Computer Science and Artificial Intelligence Laboratory, 2015

https://dspace.mit.edu/entities/publication/29dd43b7-115f-4d76-a45c-602903903194

[8] European Court of Human Rights, Podchasov v. Russia, application 33696/19, February 13, 2024

https://hudoc.echr.coe.int/eng?i=001-230854

Read the original article online

https://cybercenter.space/insights/stockholm-lawful-access-encryption-cyber-diplomacy-2026/