DIGITAL EVIDENCE IN EUROPE:

Persistent Challenges, Practical Solutions

JENNIFER DASKAL & FRANCES SCHROEDER

JUNE 2026

CENTER FOR CYBERSECURITY POLICY AND LAW

Contents

I. Executive Summary

Law enforcement increasingly depends on digital evidence to investigate and prosecute crimes but faces ongoing challenges in doing so effectively. A survey of European law enforcement officials, supplemented by qualitative interviews, breaks down these challenges. When asked to choose among a list of potential challenges, respondents identified locating relevant data sources and obtaining data once identified as their two greatest hurdles. Both ranked higher than technical difficulties of extracting data from devices or analyzing data once it had been obtained.[1]

More than half of the respondents also indicated that they almost always or frequently need access to data that requires working with entities in another country or jurisdiction. Respondents further indicated that over 60% of cross-border requests involve other European Union (EU) Member States.

These findings point to the importance — and promise — of the forthcoming implementation of the EU's e-Evidence package. Under these new rules, which enter into effect on August 18, 2026, law enforcement authorities in one EU Member State can issue preservation and production order certificates directly to a private-sector service provider located in another EU country, without having to go through the relevant country's government officials.[2] The new rules also require service providers that "offer services" in the EU to appoint a legal representative to receive and respond to such orders, even if they are not physically located in the EU.[3]

This marks a significant shift in the way European law enforcement can access digital evidence. Under the existing system, European law officials have limited options for accessing data across borders.

- The traditional route — the mutual legal assistance process — requires a government-to-government request for data; is slow and cumbersome, often taking multiple months if not longer; and is simply not built to handle the volume of requests, given the increasing importance of digital evidence to criminal cases.[4]
- Even the "simpler and faster" European Investigation Order, pursuant to which the judicial authority in one EU Member State can request the production of data located in other EU Member States, has a response deadline of four months (120 days).[5]
- As a workaround, European law enforcement officials have increasingly relied on private-sector cooperation, via voluntary disclosures of mostly subscriber information, to support their investigations.[6] But there are no EU-wide standards governing these disclosures.

The e-Evidence package provides a new way of accessing data across borders.

- The new rules set very short deadlines for responses — 10 days for an initial response in most cases and eight hours for emergency responses.[7]
- The e-Evidence package also sets procedural and substantive requirements that requesting Member States must meet for all requests, including requests for subscriber information. This standardization provides clarity, transparency, and uniformity in terms of what is required, thus eliminating some of the opacity and inconsistencies with respect to voluntary disclosures. In some cases, the rules may impose heightened procedural and substantive requirements than otherwise apply in certain national laws, thus enhancing protections for privacy and civil liberties.
- The rules also have broad reach. U.S.-based service providers and other global companies that "offer services" to EU residents are subject to the same timelines and same standards as EU-headquartered service providers.

As with any significant legal and regulatory transformation, there will be a transition period. The implementation of new rules and processes, and the shift away from voluntary disclosures to standardized processes, will require significant adjustments among Member States and providers. Effective implementation is not automatic. It will require significant investment, education, and a range of technical and operational adjustments. Public and private sector actors will need to actively support the project of transformation, in order for the e-Evidence rules to achieve their full potential.

Among the most immediate issues:

- The e-Evidence Directive required Member States to adopt implementing national legislation, pursuant to which service providers are required to designate a legal establishment or representative, by February 2026. As of June 2026, over three-quarters of Member States have not yet done so.[8] Enactment of implementing legislation is critical

to ensuring the e-Evidence package functions effectively.

- The e-Evidence Regulation mandates the development of a new information technology (IT) system that will connect Member States, EU institutions, and service providers and through which requests for digital evidence will be made and responsive information shared.[9] But the system is not yet fully functional, has gaps in terms of the amount of data it can effectively handle, and will require a significant investment in cybersecurity and other safeguards to ensure the security and privacy of the data shared through this system.
- The e-Evidence rules shift the standards, processes, and even the primary government entities given key responsibility for requesting digital evidence. Long-established processes will need to shift, new public-private relationships will need to be established, and both public and private sector entities will need to learn to use new forms and new technological systems. Effective implementation will require meaningful investment in training and ongoing support for all stakeholders involved.

This report includes detailed recommendations to address each of these issues. The report also draws on the combination of qualitative and quantitative interviews to recommend additional structural and operational shifts that would improve access to digital evidence and further support smooth implementation of the e-Evidence package.

Approach and Methodology

Digital evidence is critical to the investigation and prosecution of serious crime. Some even consider digital evidence more important than DNA and physical evidence to law enforcement's ability to successfully investigate and prosecute cases.[10] But digital evidence can be challenging for law enforcement to identify, access, analyze, and use effectively.[11] This has led to calls for decryption mandates, new data retention rules, and other legal requirements that require technology companies to design systems to facilitate law enforcement access to data. There are ongoing and active discussions about whether and how to responsibly do so.

The purpose of this project is to focus on ways to support lawful access to the significant subset of digital evidence held by third-party service providers, without relying on or waiting for new mandates to issue, and in a manner that preserves privacy, security, and civil liberties protections. The report follows the methodology used in a separate 2018 report on law enforcement access to data in the United States — but nearly a decade later, with an EU focus, and on the eve of implementation of the EU's e-Evidence package.[12]

Consistent with the approach taken in 2018, our team met with key policymakers in the EU, including at the European Commission, the European Union Agency for Law Enforcement Cooperation (Europol), and the European Union Agency for Criminal Justice Cooperation (Eurojust); hosted in-person roundtables with EU Member States' police, prosecutors, and representatives from ministries of justice and interior; and held discussions with key private sector entities and outside experts from civil society and academia. We supplemented these discussions with a survey of law enforcement officials, mostly at the managerial level, from seven countries across Europe.[13]

Key survey findings include the following:

- More than half of respondents indicated that either they or their teams work with digital evidence daily. Approximately one-third work with digital evidence at least weekly.
- More than 85% of survey respondents indicated that they need digital evidence controlled by entities in other countries in almost all or some of their cases.
- Survey respondents estimated that approximately 60% of cross-border requests involve other EU Member States and 25% involve the United States.
- About half of respondents say digital evidence is almost always or frequently encrypted; this finding encompasses encryption across multiple domains (including both devices and online services).
- Almost three-quarters of survey respondents indicated that they are ultimately able to access encrypted data or find workarounds approximately half of the time or more.[14]
- More than one-third of respondents indicated that they did not feel adequately trained to confidently handle digital evidence.

II. Background: Law Enforcement Challenges and Operational Needs

According to a 2018 study conducted by the EU, some 85% of criminal investigations involve the use of digital evidence; quantitative and qualitative results suggest that the percentage may be even higher as of 2026.[15] This is not surprising. The ubiquity of digital devices, sensors, communications platforms, and storage systems means that just about every human action — including criminal acts — leaves a digital footprint. Some scholars have called this the "golden age of surveillance."[16]

Yet, despite this, it can be quite difficult for law enforcement to obtain and use digital evidence to investigate and prosecute crime, even when there is a lawful basis for doing so. The dizzying array of service providers and technologies makes it challenging for law enforcement officials to know where to find sought-after digital evidence. Jurisdictional hurdles make it hard to obtain digital evidence, even if there is clarity about where to find it. And once obtained, it can be hard for law enforcement to understand, interpret, and use effectively. In fact, the sheer scale of information can make it harder to manage. The simple task of sorting and analyzing, determining what is relevant and what is not, requires training and skill.

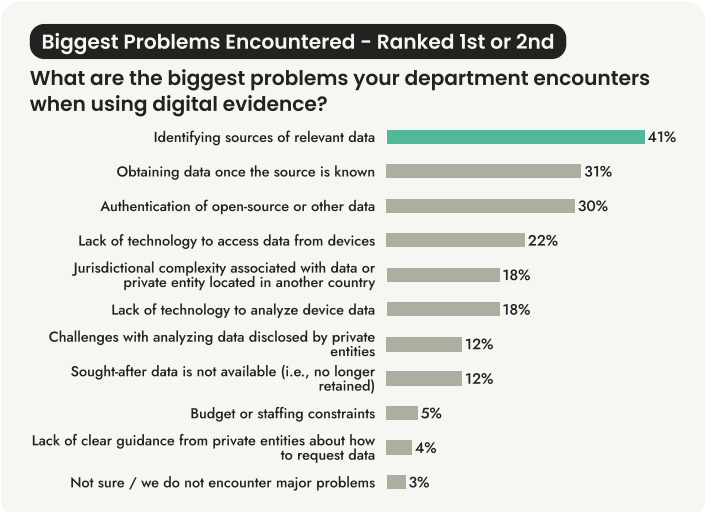
The following section starts with a short description of the scope and scale of digital evidence, and then describes the core challenges, as reported by law enforcement, in obtaining and using digital information.

What is Digital Evidence?

Digital evidence comes in a variety of forms and can be obtained from an array of sources, including devices (such as phones and laptops), open-source information, surveillance videos, and service providers (such as social media companies, email service providers, and telecommunication providers).

The bulk of this report focuses on this final category – the large amount of data that is held and controlled by service providers. Such data is generally broken down into three key categories: subscriber data, traffic data, and content data. Subscriber data is often used for identification purposes, and includes information related to a user's subscription to a given service, such as registered name, address, billing and payment information, telephone number, or email address. Traffic data includes metadata related to the provision of a service, such as time, date, and location of use, log-in history, and source and destination of a message, and is often helpful for identifying or establishing presence at a particular place at a particular time. Content data includes the substantive content of communications, such as text, voice, videos, and images.[17] Each can serve valuable law enforcement purposes in the investigation and prosecution of crime.

Challenges Identifying and Obtaining Relevant Data



Both survey respondents and qualitative interviews highlighted the challenges in identifying and obtaining digital evidence for use in their cases. When survey respondents were asked to rank the challenges encountered by their department when using digital evidence, 41% ranked "identifying sources of relevant data" and 31% ranked "obtaining data once the source is known" as among their top two challenges. Of note, this question addressed digital evidence challenges writ large; it was not limited to digital evidence in the hands of service providers.

Interviews in both Sweden and the Netherlands suggested some practical ways to support law enforcement officials, via the sharing and pooling of expertise.

Sweden

Sweden has established a National Cybercrime Center (called SC3), with regional branches, where law enforcement can obtain technical support and training. Structured to mirror Europol's European Cybercrime Centre (called EC3), SC3 supports the investigation of complex cybercrime, provides technical support and training to law enforcement across Sweden, and coordinates with private sector and international partners, including through regular engagement with Europol. It is located within the Swedish Police Authority's National Operations Department.

SC3 employs specific subject matter experts to support the national police and inform relevant policies and legislation. In complex cybercrime investigations, SC3 works with and supports specialized prosecutors who can obtain court orders on mutual legal assistance.

Currently, SC3 also serves as the single point of contact for government-to-government and government-to-private sector engagement for digital evidence, which helps centralize knowledge about where to pursue sought-after data and how to do so.

By concentrating expertise and developing ongoing working relationships with key service providers, SC3 is credited with improving the quality of requests and achieving high success rates, in terms of percentage of requests for evidence that result in disclosures.[18]

The national-level SC3 is supplemented with seven regional cybercrime centers (RC3s), which support local law enforcement. The regional centers are the first point of contact for local investigators, providing hands-on case support. SC3 develops specialized training that is then disseminated through the regional centers.

The Netherlands

The Netherlands similarly has put in place structures to facilitate specialized expertise on digital evidence.

In the Netherlands, the Public Prosecution Service, made up of approximately 800 public prosecutors, is responsible for overseeing the execution of investigations, determining which cases to pursue, and approving the investigative methods that are employed. The prosecution service has developed specialized expertise in digital investigations, to include the appointment of a National Public Prosecutor for Digital Investigation, a National Prosecutor for Cybercrime, and prosecutors dedicated to cybercrime appointed to district offices across the country. [19]

The police service has similarly invested in building out the capacity to handle digital evidence and complex cybercrime cases. The National High-Tech Crime Unit handles complex cases involving digital evidence, engages with international partners, and supports police across the country by sharing its operational expertise on digital evidence.[20] The Netherlands Forensic Institute, housed within the Ministry of Justice and Security, supports efforts to access digital evidence and provides training to law-enforcement personnel.[21]

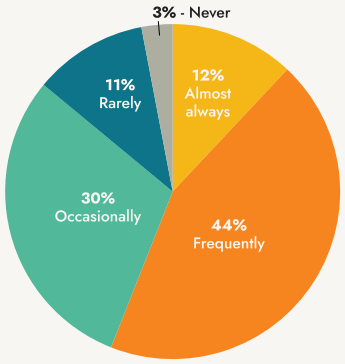
Each region is supported by teams of police and detectives trained in digital evidence.

Cross-Border Complications

The EU estimates that, as of 2018, 55% of criminal investigations involved a cross-border request for data from a service provider located in another jurisdiction.[22] In our 2026 survey of European law enforcement, 86% of survey respondents indicated that they occasionally, frequently, or almost always need to work across borders to access digital evidence; 56% indicated that they almost always or frequently have this need. The majority of those requests require working with other countries within the EU. Survey respondents estimated that, on average, approximately 60% involve requests for evidence from an entity in another Member State; 25% involve the United States, and the rest involves other regions of the world.

Frequency of Cross-Border Data Requests

How often do you seek access to data from an entity located in another country or jurisdiction?



86%

almost always, frequently, or occasionally need access to data from an entity across borders.

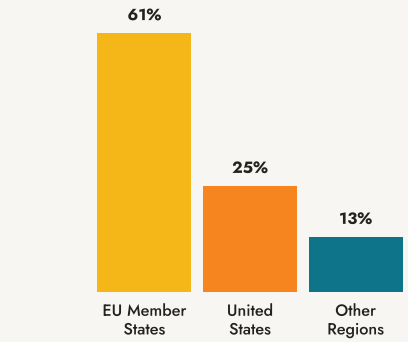
Survey responses and separate qualitative interviews described multiple challenges in dealing with these cross-border requests. Key challenges include conflicts of law, delays in getting sought-after data, chain of custody or authentication concerns, and difficulty identifying which provider holds the data.

The soon-to-be implemented e-Evidence package offers potential solutions to many of these challenges. Among other things, it will minimize the risk of legal conflicts among EU Member States and set clear rules, applicable across all of the EU, for obtaining sought-after information.

A U.S.-EU CLOUD Act Agreement, discussed in more detail below, is also needed to address potential conflicts of laws for those providers subject to both EU and U.S. law, and streamline the process for obtaining data from companies subject to U.S. jurisdiction.[23]

Share of Cross-Border Requests by Region

Of cross-border requests for digital evidence, roughly what share are directed to each of the following regions?



International Coordination: Europol & Eurojust

Complex cases involving digital evidence, such as ransomware, drug trafficking, and child exploitation cases, often involve multiple jurisdictions. The European Union Agency for Law Enforcement Cooperation (Europol) and the European Union Agency for Criminal Justice Cooperation (Eurojust) provide critical support to law enforcement and judicial authorities on such cases.

Europol

Europol serves as a hub for international law enforcement authorities to co-locate and collaborate on multi-state investigations.[24] Europol brings together foreign liaison officers and investigators, offers operational and analytic support on specific cases, and pools resources.

Europol's European Cybercrime Centre (EC3) specifically focuses on cybercrime investigations. EC3 facilitates joint law enforcement operations and provides highly specialized digital forensic and strategic support. EC3 also provides highly specialized trainings, including workshops on cryptocurrency demixing and decryption.

Europol also houses the permanent Joint Cybercrime Action Taskforce (J-CAT), a standing operational team that coordinates cross-border investigations into and operational actions against key high-profile cybercrime threat actors.[25]

Eurojust

Eurojust performs a parallel function for prosecutors and other judicial counterparts by supporting judicial coordination across the EU and with other international partners in cases involving serious organized crime and terrorism.[26] Eurojust provides both strategic and operational support, coordinates multilateral investigations and prosecutions, and helps resolve cross-border jurisdictional conflicts.

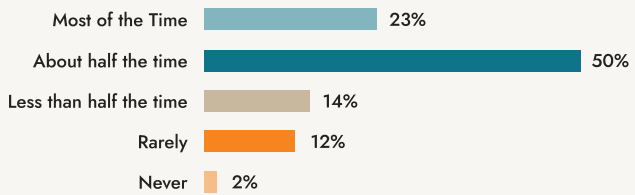
Technical Challenges

Technical challenges related to digital evidence span an array of issues, from the ability to obtain data from devices to deciphering data that has been obtained. In our roundtable discussions, officials raised concerns about data retention, noting that electronic content subject to a request for digital evidence from a law enforcement authority may no longer be retained.

Survey results and roundtable discussions also delved into challenges posed by encryption. As described above, both survey results and separate qualitative discussions indicate that law enforcement regularly encounter encrypted data. But 73% of survey respondents indicated that they are ultimately able to access that data or find workarounds approximately half of the time or more.[27]

Success Accessing Encrypted Data

When data is encrypted, how often are you ultimately able to successfully decrypt the data or find alternative sources that are not encrypted?



73%

are able to successfully decrypt data most of the time or about half the time

Training and External Support

Training and external support are critical to enabling law enforcement to effectively access and interpret digital evidence. Yet, more than one-third of respondents indicated that they did not feel sufficiently trained to confidently access, interpret, and use digital evidence in their cases.

Given the complex and varied nature of digital evidence and resource constraints, law enforcement often turns to outside sources for support on digital evidence. Such external support comes from entities including national forensic units, liaison teams of service providers, EU-level agencies such as Europol or Eurojust, and private consultants. These training opportunities provide important supplements to national level training and support — which will be particularly essential as Member States transition to using the new e-Evidence processes, standards, and technologies.

EU-Wide Training Resources

Training will be key to unlocking the potential of the e-Evidence package. It is also key to supporting the lawful use of digital evidence more broadly. Training will only become more important over time, as prosecutors and law enforcement work through the challenges posed by and learn to leverage the potential of artificial intelligence.

Several EU-level entities already serve important training functions. These entities should be resourced and supported to continue this work and to support Member States with the transition to the e-Evidence regime.

Some of the key entities include:

- *The European Judicial Cybercrime Network (EJCN):* EJCN brings together judicial practitioners across Member States focused on cybercrime and digital investigations to exchange expertise related to emerging challenges with digital evidence and cyber-enabled crime.[28] EJCN also provides training for judicial entities, including "master classes" and other specialized trainings.
- *The European Judicial Training Network (EJTN):* EJTN is a nonprofit funded by the EU that promotes training and knowledge exchange among judicial authorities across Member States.[29] EJTN organizes judicial training and seminars, runs exchange programs, including specialized exchanges on the "digitalisation of justice" and cybercrime, and supports coordination across other training institutions.[30]
- *The European Union Agency for Law Enforcement Training (CEPOL):* Headquartered in Budapest, CEPOL is an EU-funded entity that works with national law enforcement academies across the EU to coordinate training, develop curricula, and facilitate the exchange of information.[31]
- *The European Cybercrime Training and Education Group (ECTEG):* ECTEG is a non-profit funded by the European Commission to develop online and on-site training courses for law enforcement on the use of electronic evidence.[32]
- *The SIRIUS Project:* Europol and Eurojust jointly run the SIRIUS project, which hosts an online platform available to law enforcement and judicial entities to exchange best practices, advice, and other practical information for dealing with cross-border digital evidence.[33] This includes contact information for service providers, training materials, and guidelines on lawfully requesting content from specific providers in cross-border cases. While the current phase of the SIRIUS project is focused externally, outside of Europe, the project is a repository with a wealth of information for Member States looking to enhance practices related to cross-border access to data, both within the EU and beyond.

Several service providers also offer training and briefings for law enforcement, contribute to the SIRIUS Project, and support broader training efforts.

III. The Potential of e-Evidence

The EU's new e-Evidence package will go into effect on August 18, 2026. The new rules — which consist of a regulation and directive — are designed to expedite and harmonize the process by which law enforcement and judicial authorities in the EU can obtain electronic evidence from a service provider located in another Member State.

By establishing a streamlined framework for direct cross-border production and preservation orders, e-Evidence promises to dramatically transform the process and speed by which European law enforcement can access sought-after data across EU borders. As described above, existing mechanisms for accessing data across borders have struggled to keep pace with the volume and complexity of law enforcement investigative needs.

If implemented as intended, e-Evidence will support a more predictable, timely, and effective process for law enforcement officials across the EU to lawfully obtain digital evidence from service providers located in other EU Member States. It will also give law enforcement officers new jurisdiction over providers that "offer services" in the EU, even if they are not physically located there. This would significantly strengthen European law enforcement's ability to lawfully access and use digital evidence.

But as with any new legal regime, there are several implementation challenges, each of which needs to be worked through, in order for e-Evidence to have the effect that is intended:

- Each Member State is required to pass new laws to "transpose" the e-Evidence Directive — which sets out the requirements that service providers designate a representative or establishment — into national law. Only a fraction of the EU Member States has done so.
- Law enforcement and judicial authorities will need to learn entirely new standards, processes, and systems.
- Service providers also need to learn and apply new rules governing what and how information is to be provided.
- The system will operate on a newly developed, decentralized IT system that still needs to be implemented and that has capacity limits. As with the development of any new IT system, there are significant technical, security, and operational challenges to work through.

There also is some risk that the new rules could exacerbate, rather than minimize, conflict of law concerns for U.S.-based providers that offer services in the EU and will be subject to both e-Evidence and separate U.S. rules governing the disclosure of certain communications content to foreign law enforcement. There is a corresponding need for a U.S.-EU agreement — presumptively in the form of a U.S.-EU CLOUD Act Agreement — to clarify the respective rules and obligations and minimize the risk of such conflict.

The following provides a summary of the e-Evidence package and then delves into these challenges, along with proposals for addressing them.

The e-Evidence Regulation

The e-Evidence Regulation establishes new mechanisms by which authorities in one Member State can issue a European Production Order Certificate (EPOC) or European Preservation Order Certificate (EPOC-PR) directly to a service provider in another EU Member State for digital evidence.[34]

Under current law, law enforcement in one Member State cannot directly compel a service provider located in another Member State to provide sought-after data. Instead, law enforcement must make a government-to-government request for the data, or, alternatively, rely on voluntary cooperation by service providers. Response times to government-to-government requests are generally long. Even the reportedly "quick" European Investigation Order — pursuant to which a judge in one EU Member State can make a binding request for another Member State to assist in the gathering of digital evidence for use in a criminal prosecution — allows for a 120-day response time.[35]

By contrast, response deadlines under the e-Evidence Regulation are short. Service providers must respond to production orders within 10 days for ordinary requests, and within eight hours for emergency cases.[36] Preservation orders require that specified electronic evidence be preserved "without undue delay" for a 60-day period.[37] Those that fail to comply with these requirements, absent a valid ground for refusal, are subject to potential penalties.[38]

The procedural and substantive requirements depend on the type of data being sought. Data is categorized as follows:

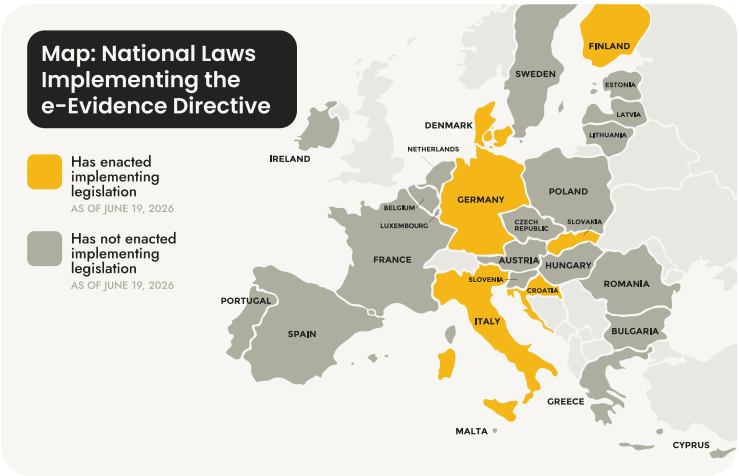
- *Data requested for the sole purpose of identifying the user* — IP addresses and, where necessary, date, time stamps, or technical equivalents when requested for the sole purpose of identifying the user in a specific criminal investigation;
- *Subscriber data* — Data relating to the subscription of a service, pertaining to: (a) the identity of a subscriber or customer (i.e., name, date of birth, postal or geographic address, billing and payment data, telephone number, or email address) or (b) the type of service and its duration;
- *Traffic data* — Data related to the provision of a service, such as device location data, time of use, source and destination of a message, and other electronic communications metadata relating to the commencement and termination of a user's access to a service, such as the date and time of use;
- *Content data* — Text, voice, videos, images and sound, and other data in a digital format that is not subscriber or traffic data.[39]

Procedural and substantive requirements vary based on whether a request involves: (i) data being obtained for purposes of identifying the user or subscriber data (what we are calling "Category One" data), or (ii) traffic or content data ("Category Two" data).

- *Issuing Authority* — Production orders for Category One data can be issued by a judge, court, investigating judge, or public prosecutor, or another state-identified competent authority, subject to validation by a judge, court, investigating judge, or public prosecutor. For Category Two data, only a judge, court, or investigating judge can issue or validate orders; public prosecutors cannot.[40]
- *Scope of Covered Offenses* — Production orders for Category One data can be issued for all criminal offenses; production orders for Category Two can only be issued for criminal offenses with a maximum sentence of at least three years and other specified offenses.[41]
- *Procedural Requirements/Engagement with Other Member States* —When seeking Category Two data, the requesting Member State needs to inform the "enforcing authority" — meaning the governmental authority in the state where the order is being sent, unless an exception applies.[42] The enforcing authority then has ten days to object to ordinary requests, and 96 hours to object to emergency requests.[43] This requirement to engage with the enforcing authority in the recipient Member State does not apply to Category One data.

All production and preservation orders, whether Category One or Two, must meet the requirements of necessity and proportionality and must include underlying information regarding the basis for determining that the order meets the requirements of necessity and proportionality.[44]

The e-Evidence Directive



The Directive mandates that each Member State adopt implementing national legislation that: (i) requires service providers offering services in the EU to appoint a designated establishment or legal representative to receive production and preservation orders under the Regulation;[45] and (ii) imposes penalties on those service providers that fail to do so.[46] Each Member State is also required to designate at least one "central authority" to oversee enforcement of the Directive.[47]

The deadline for complying with the Directive was February 18, 2026. As of June 19, only Croatia, Denmark, Finland, Germany, Italy, and Slovakia have adopted such implementing legislation.[48] The European Commission has initiated infringement procedures against the many EU Member States that failed to meet the Directive's deadline, giving them two months from the end of March 2026 to comply.[49]

Ireland

Hundreds of service providers are expected to appoint their legal representative or designated establishment in Ireland. This will include several of the large U.S.-based service providers. As a result, Ireland anticipates that a large volume of production orders — namely, more than 300,000 production orders a year — will be issued to providers in its country.[50]

Ireland has established a Criminal Justice International Cooperation Office, which will serve as the notification and enforcing authority for e-Evidence orders, but has not yet transposed the Directive into Irish law. Service providers can still register in Ireland, but they are not required to do so until the implementing law is in place. As of June 2026, Ireland's implementing legislation is under consideration by the legislature, but not yet law.[51]

Adding additional complexity, Ireland also has not yet opted into the separate European Investigation Order (EIO) Directive, although Ireland has indicated it ultimately intends to do so. In the short term, this creates an additional challenge. Service providers that intend to designate in Ireland will need to designate two different representatives: one for e-Evidence orders (which could be in Ireland), and one for orders under the EIO Directive (any Member State other than Ireland or Denmark). Ireland is reportedly working to transpose the EIO Directive and opt in to the procedure, but it is not expected to do so before August 2026.[52]

Given the central role that Ireland will play in e-Evidence implementation, it is important that Ireland act quickly to transpose both the e-Evidence Directive and EIO Directive as soon as possible. Ireland also should focus efforts and resources on ensuring that its technical infrastructure can handle a large volume of requests, and that its Criminal Justice International Cooperation Office, which will be responsible for reviewing requests for traffic and content data, is adequately staffed with the personnel and expertise to effectively manage the high volume of cross-border orders.

The New IT System

The e-Evidence Regulation requires that the exchange of forms, data, and other communications under e-Evidence be transmitted through a newly developed "secure and reliable decentralised IT system" used to connect Member States, EU entities, and service providers.[53]

Cross-border communication will be facilitated through the pre-existing "backend" message transport infrastructure known as "e-CODEX." e-CODEX is used to securely exchange legal data and documents between Member States.[54] The e-CODEX transmission infrastructure, however, is subject to a capacity constraint, which limits the size of data that can be transmitted through the system. Even when fully functional, it will not support the transfer of data more than 25 megabytes — which will ultimately require workarounds for the transmission of most content and traffic data. [55]

The Regulation gives the European Commission the task of developing multiple new elements of this system, including:

- A new "reference implementation software" — a front-end software system that can be used to create requests for data, send and receive messages, and manage workflows and forms.[56] Member States, however, are not required to use this system. Member States can instead develop their own software to access the system and make requests to service providers, so long as they meet certain technical standards. In July 2025, the Commission adopted an Implementing Regulation setting out the technical requirements for Member State systems.[57]
- The specifications for a common application programming interface (API), to be shared with service providers via Member States, which will provide a means of accessing the Member States' decentralized IT systems. The common API is required "to the extent possible and reasonable" to be based upon the technical specification developed by the European Telecommunications Standards Institute.[58]
- A new court database, which will serve as an authoritative list of relevant points of contact, including service providers' designated establishment or legal representative and Member States' competent authorities. The Commission is directed to make access to this database available via an API provided to competent authorities, Eurojust and the European Public Prosecutor's Office.[59]

Service providers are required to ensure that their designated establishment or legal representative can connect to the Member States' IT systems. Service providers can either use the European Commission-developed interface or develop bespoke IT infrastructure to receive and respond to requests for digital evidence.[60]

The Member States and EU entities are responsible for the cost of installing, operating, and maintaining the components of the system under their responsibility. Service providers are responsible for costs necessary to integrate with the system.[61]

The e-Evidence Regulation also recognizes that there may be moments where the system is not operable, in which case Member States are instructed to use the "most appropriate alternative means" for sending requests and responses.[62] These alternative means will be required for any responses that exceed the e-CODEX capacity limitation.

IV. Outstanding Challenges for e-Evidence Implementation

The following delves into some of the outstanding challenges with implementation — along with proposed solutions.

Incomplete Transposition of Directive into National Laws

Under the Directive, Member States were required to transpose the Directive into national law by February 18, 2026. But fewer than half have done so. This is a critical element of the package. It is the mechanism by which all service providers are required to designate representatives to receive requests for data and preservation orders.

Recommendation to Transpose the Directive Promptly

Member States should act quickly to transpose the Directive into their national legislation as soon as possible, ideally before August 18, 2026. Covered service providers should ensure that they act promptly to appoint their designated establishment or legal representatives once the relevant laws are in place.

Technology and Cybersecurity Challenges

The e-Evidence package requires implementation of a new technology system by entities across the EU. While the backbone of this system uses the existing e-CODEX infrastructure, the Regulation requires the development of a new "reference implementation software" by the European Commission. Member States are encouraged but not required to use this software, and can instead adopt their own implementation software, consistent with the technical standards defined in the Implementing Regulation.

Developing and implementing new IT systems is challenging. New systems often face early-stage bugs, technical flaws, and other operational issues.[63] Emerging AI tools and other technological developments exacerbate these inherent security challenges, as they make it easier for even unsophisticated bad actors to identify targets, write malicious code, and exploit vulnerabilities.[64]

Among the key cybersecurity and technical challenges:

- **Complexities and Cybersecurity Risks Resulting from a Multi-State, Interconnected System —** Member States are responsible for operating and maintaining their national IT system and access points to the broader EU-wide system. If they use the Commission-developed reference implementation software, the software will be provided and maintained by the Commission, free of charge. If they do not, they will need to develop and maintain all aspects of the system.[65]

  The overall security of the framework is affected by decisions made by the Commission, each Member State, and any other entities (i.e., Eurojust, the European Public Prosecutor's Office) connected to the system. Of particular concern, vulnerabilities in one system can be exploited in ways that affect the wider network. In other words, the system is only as good as its weakest link. It is critical that every part of the system invest in ensuring effective cybersecurity, to include a combination of effective technical controls, vulnerability management, auditing, and governance structures. Variations in preparedness and technical sophistication across Member States can create cybersecurity risks that extend beyond each State's borders.

- **Encryption Standards —** The Implementing Regulation allows, but does not require, issuing authorities to include an X.509 public key certificate with the requests to produce data.[66] An X.509 public certificate is important: it enables asymmetric encryption of transmitted data. This is a much more secure system of transmitting data, as compared to symmetric encryption. With symmetric encryption, both parties exchange and use the same key. By contrast, asymmetric encryption uses a pair of keys, each held separately, eliminating the need to transmit a sensitive shared key. Even this, however, is a short-term measure. Ultimately, Member States should employ quantum-resistant encryption, so that data collected now is not decrypted later, as quantum capabilities mature.

- **Cybersecurity Risks Related to Size Constraint —** As described above, the decentralized IT system will not transmit files larger than 25 megabytes. In many cases, files that include content and traffic data will exceed this capacity constraint. In such situations, service providers and competent authorities will be required to share data through "alternative" means, outside of the validated IT system, and without the required application of the technical safeguards laid out in the Implementing Regulation.[67]

  Large service providers that are accustomed to receiving law enforcement requests for data have existing portals to receive and respond to law enforcement requests for data; these will presumably serve as the alternative means for receiving and transmitting requests. But not every service provider that might be subject to a request for data has such a system in place, and the lack of uniformity risks inconsistent levels of protection, undermining overall cybersecurity.
- **Access Controls & Governance —** The system only works if requests are sent from legitimate issuing authorities and the responses are transmitted back to those same legitimate authorities—without being maliciously diverted. Secure access controls, effective authentication, and governance systems to protect against unauthorized access to the system are vital, including for requests and responses transmitted through alternative means outside of the decentralized IT system. Each participant in the process also has responsibility to ensure that the requests are valid and the responsive data is sent to an authorized, legitimate user from the requesting State.

Recommendation to Prioritize Cybersecurity

The Implementing Regulation establishes a technical framework for the decentralized IT system, yet key details are left to Member States and other entities that connect to this system. The European Commission and Member States should leverage existing cybersecurity expertise at the EU-level, including the European Union Agency for Cybersecurity (ENISA) to ensure that the implementation of effective technical controls, vulnerability management, and governance systems to ensure the security of the system.

- The Commission should prioritize rigorous testing of the decentralized IT system, including stress testing the system with edge cases, high-volume requests, and other real-world use cases to identify and address weaknesses.
- As Member States set up infrastructure to issue and enforce orders, they should implement robust testing, auditing, and governance mechanisms. This includes conducting regular security audits, continuous monitoring, implementation of clearly defined response procedures, mechanisms for rapid mitigation and recovery, and validation of interoperability with the EU-wide system.
- Data will need to be exchanged through alternative channels if responsive information exceeds the system's 25 megabyte capacity limit or if the system is otherwise unavailable. Member States and service providers should agree in advance on secure fallback channels that meet consistent security requirements for transferring data. These procedures should be tested to ensure reliability.
- Member States and service providers should agree on clear authentication procedures for transmissions outside of the system for both the requesting authority and recipient, such as only using pre-validated official contact points.
- Member States should require that all issuing authorities use a X.509 public key certificate to asymmetrically encrypt requests for data. (This is something that the Implementing Regulation supports but does not require.) However, even X.509 certificates are only a short-term protection. Ultimately, Member States should implement – and require – the use of quantum-resistant encryption. This will reduce the risk that sensitive law enforcement data can be collected now and decrypted later as quantum capabilities mature.
- Each Member State and the Commission should establish and clearly communicate the lines of responsibility for ensuring strong cybersecurity of the system and dealing with incidents when they occur.
- Each Member State should identify a dedicated cybersecurity entity or official responsible for addressing vulnerabilities and other cybersecurity concerns, and for updating authentication and access procedures as technologies and associated threats evolve.
- Responsible officials should regularly convene to share information and address potential and known vulnerabilities. This kind of information sharing, coupled with clarity about responsibility and roles, is critical to effective risk management.

Transition to Full Implementation

Given the incomplete status of Member States' transposition of the Directive into national laws, in addition to varying levels of technical preparedness across Member States, it is likely that there will be a phased implementation of the e-Evidence package. To ensure law enforcement maintains the ability to access digital evidence to investigate and prosecute crime, it is important that all parties involved take steps to avoid major disruptions during the transition.

Recommendation to Minimize Disruptions During a Period of Implementation

All cross-border law enforcement requests for data to service providers should eventually be handled through the rules and procedures laid out in the e-Evidence package. But there will be a transition period. To protect against disruption to ongoing investigations and prosecutions, currently approved mechanisms for sharing data, such as voluntary disclosures of certain non-content data, should continue until the system is in place and fully operational.

Need for Training

The e-Evidence package establishes new rules, new international coordination mechanisms, new forms, new IT systems, and new opportunities to obtain or to preserve data from service providers operating in the EU. There will be a learning curve. The European Commission and EU agencies, such as Europol and Eurojust, have already hosted some trainings and more have been announced. But capacity is limited and there are many entities, law enforcement officials, judges, and service providers who will need to learn the new rules and processes, and much more training is needed.

Recommendation on e-Evidence Training and Ongoing Support

The European Commission and Member States should work together, and in collaboration with key partners, such as the European Judicial Training Network, to support what will need to be ongoing efforts to train both judicial and law enforcement authorities on the processes, standards, and ways to best operationalize the new rules. Training should cover the legal framework, the procedural requirements, and the technical and operational components for effective implementation. Training should be made widely available via a combination of "train the trainer" efforts and online tools. Member States should implement centralized resource centers to support local investigators and prosecutors as new issues emerge.

Service providers should take advantage of the Commission-offered "train the trainer" sessions and also develop mechanisms to share relevant information with those tasked with handling the execution of orders under e-Evidence.

Ongoing Conflict of Law Concerns

The e-Evidence rules require providers that offer services in the EU to produce data in response to lawfully issued production orders, even if they are not physically located in the EU. Failure to do so can result in significant penalties—up to 2% of a provider's total worldwide revenue from the preceding financial year.[68]

Conversely, the U.S.'s Electronic Communications Privacy Act (ECPA) prohibits the disclosure of content data to foreign government entities, absent an applicable exception.[69] These contradictory legal requirements create the risk that service providers will be caught in a conflict of laws — required to disclose data relevant to a European criminal investigation or prosecution but prohibited from doing so under U.S. law.

The e-Evidence Regulation anticipates the possibility of legal conflict and sets up a process for providers to raise conflict of law concerns and seek review by an EU court.[70] But the outcome of those challenges is uncertain. Moreover, the pronouncement of an EU court might not match the views of a U.S. judge. This puts service providers in an unreasonable situation: having to choose between potential fines under e-Evidence for failing to comply with production orders or potential liability in the United States for engaging in unlawful disclosures.

There are ways around such conflicts. Providers can, for example, rely on user consent for disclosures mandated under EU law. Or they can design their systems in such a way that Europeans' data is treated as subject to EU law, whereas other data is treated as subject to U.S. law. But there is still uncertainty. The EU and United States should take steps to provide clarity as to whose rules apply in what circumstances.

Recommendation for a U.S.-EU CLOUD Act Agreement

To protect against legal conflict, the EU and United States should restart stalled discussions on a Data Sharing Agreement pursuant to the U.S. CLOUD Act.[71]

The CLOUD Act addresses conflict of law concerns. It authorizes the U.S. government to enter into an executive agreement with foreign governments, pursuant to which the foreign government can directly compel the production of non-U.S. person data from a U.S.-based service provider, subject to baseline substantive and procedural requirements.[72]

There are currently two CLOUD Act Agreements in place: one with the United Kingdom and one with Australia.[73] While negotiations on a U.S.-EU CLOUD Act Agreement began with the EU in 2023, they have reportedly stalled.[74]

A U.S.-EU CLOUD Act Agreement could help minimize conflicts of law, clarify expectations as to when U.S.-based providers are expected to comply with EU production demands, and ensure continued protections for Americans' data, consistent with what is required by ECPA.

A U.S.-EU CLOUD Act Agreement could also explicitly address other potential conflict of law issues, including those that stem from a potential clash between U.S. production orders and Article 48 of the EU's General Data Protection Regulation, which places restrictions on data transfers.[75]

A U.S.-EU CLOUD Act Agreement could also address situations that fall outside of the e-Evidence framework – i.e., when EU law enforcement seeks content from a provider subject to U.S. law that does not "offer services" in the EU and is not subject to the e-Evidence requirements. An Agreement would help fill this gap.

V. Broader Recommendations

The following recommendations supplement the more specific recommendations focused on e-Evidence implementation—highlighting additional ongoing areas for improvement.

Strengthen Centralized National Structures

Member States should establish centralized national structures for digital evidence within law enforcement to provide operational coordination and technical expertise. Both the Swedish Police Authority's National Cybercrime Center and the Netherlands Forensic Institute offer useful examples, exemplifying how centralized national structures can support regional and local law enforcement. Centralized structures should be sufficiently resourced and designed to support local operational needs.

Build Effective Public-Private Partnerships

The e-Evidence package formalizes the process by which Member States can request information from service providers. But it does not address other core challenges: ensuring that the requests for information are both reasonable and actionable and directed at the appropriate service provider. The EU, Member States, and service providers should increase their investments in workshops and other engagements so as to build knowledge that will in turn increase the quality and effectiveness of requests for data.

Enhance International Cooperation

Complicated cases frequently require cooperation across Europe to effectively investigate and prosecute crime. The EU and Member States should increase their investment and engagement with effective multi-state entities, such as Europol and Eurojust, that provide critical support in investigating and prosecuting sophisticated cross-border crimes.

VI. Conclusion

The e-Evidence package provides a meaningful opportunity to improve and standardize the process for lawfully accessing and preserving digital evidence in the EU. To fully benefit from its promise, EU officials, Member States, and service providers will need to work together to learn a new system, train key participants as to how it works, and support the secure development of an entirely new technology system. Doing so will require ongoing investments in training, cybersecurity, and new operational structures. This report urges the EU, Member States, and service providers to make these investments now – and help ensure the success of the system.

CENTER FOR
CYBERSECURITY
POLICY AND LAW

About the Center

The Center for Cybersecurity Policy and Law is a nonprofit 501(c)(6) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry, including members of civil society and government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices.

To learn more about the Center and our wide-ranging initiatives, please visit https://centerforcybersecuritypolicy.org.

Endnotes

[1] The survey, which was conducted by the research firm Kantar between November 2025 and March 2026, included a sample of over 100 law enforcement officials across France, Germany, Italy, the Netherlands, Spain, and Sweden. The survey also included responses from five respondents in the United Kingdom. The majority of respondents held a managerial-level role or above; their responses reflect the aggregated experiences and perspectives of the personnel that they manage. Based on the sample size and an estimate of 1.6 million law enforcement authorities across Europe, Kantar calculated a maximum ±1.31 margin of error at the 95% confidence level.

[2] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *Official Journal of the European Union* L 191/118, July 28, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1543 (hereinafter "e-Evidence Regulation"); Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *Official Journal of the European Union* L 191/181, July 28, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023L1544 (hereinafter "e-Evidence Directive").

[3] e-Evidence Regulation, art. 2(1); e-Evidence Directive, art. 3.

[4] European Commission, *Commission Staff Working Document: Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, Apr. 17, 2018, at 25, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118 (hereinafter "Impact Assessment").

[5] European Union Agency for Criminal Justice Cooperation (Eurojust), "European Investigation Order," https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order.

[6] Under U.S. law, voluntary disclosures of communications content to foreign government entities are generally prohibited; these prohibitions do not apply to non-content information. See 18 U.S.C. § 2702.

[7] e-Evidence Regulation, arts. 10, 12.

[8] On March 26, 2026, the European Commission opened infringement proceedings against Austria, Belgium, Bulgaria, Cyprus, Czechia, Estonia, Finland, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovenia, Spain, and Sweden. European Commission, "Commission takes action to ensure complete and timely transposition of EU directives," Mar. 26, 2026, https://ec.europa.eu/commission/presscorner/detail/en/inf_26_679.

[9] e-Evidence Regulation, arts. 19, 23.

[10] "Survey Says Digital Evidence is Now More Important than DNA," *Forensic*, Nov. 18, 2022, https://www.forensicmag.com/592150-Survey-Says-Digital-Evidence-is-Now-More-Important-than-DNA/.

[11] *See, e.g.,* Eurojust and Europol, *Common Challenges in Cybercrime - 2024 review by Eurojust and Europol*, Publication Office of the European Union, 2025, https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf.

[12] William A. Carter and Jennifer C. Daskal, *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, Center for Strategic and International Studies, July 2018, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf. The e-Evidence package establishes new procedures for law enforcement and judicial authorities in the European Union to order access to and preservation of digital evidence. European Commission, "E-evidence," Jan. 21, 2025, https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime/e-evidence_en.

[13] See footnote 1 for a discussion of the survey sample, margin of error, and confidence level.

[14] The survey asked respondents how often they are able to decrypt encrypted data that they encounter in their work or successfully locate alternative, unencrypted sources. Responses did not distinguish between these outcomes or provide additional disaggregation with respect to data types.

[15] *Impact Assessment* at 14.

[16] *See, e.g.,* Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,* W. W. Norton & Company, 2015; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019.

[17] These definitions track those included in the e-Evidence package. See e-Evidence Regulation, art. 3(9), (11), (12). The e-Evidence Regulation further defines content data to include any data in a digital format that is not subscriber or traffic data. Id. art. 3(12). The e-Evidence Regulation also defines a category of "data requested for the sole purpose of identifying the user" in specific criminal investigations, which can include IP addresses, source ports and time stamps. Id. art. 3(10).

[18] Europol and Eurojust, *SIRIUS EU Electronic Evidence Situation Report 2024*, Nov. 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf (describing a 90% success rate in data disclosures, the highest in all of the EU).

[19] *See* Public Prosecution Service, "Netherlands Public Prosecution Service," https://www.prosecutionservice.nl/organisation/netherlands-public-prosecution-service; G. Odinot, M.A. Verhoeven, R.L.D. Pool, and C.J. de Poot, *Organised Cybercrime in the Netherlands: Empirical Findings and Implications for Law Enforcement*, 2017, at 17-19, (describing organization of investigations and prosecutions in the Netherlands), https://repository.wodc.nl/bitstream/handle/20.500.12832/179/Cahier_2017-1_Full_text_tcm28-244615.pdf.

[20] Government of the Netherlands, "Investigation and prosecution of criminals," https://www.government.nl/topics/crime-and-crime-prevention/investigation-and-prosecution-of-criminals .

[21] Netherlands Forensic Institute, Ministry of Justice and Security, "About NFI," https://www.forensischinstituut.nl/en/about-nfi.

[22] *Impact Assessment* at 14.

[23] Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115–141, div. V, § 105, 132 Stat. 1213, 1217–1225 (2018) (establishing a framework for the United States to enter into bilateral executive agreements regarding cross-border access to electronic evidence) (codified at 18 U.S.C. § 2523) (hereinafter "CLOUD Act").

[24] Europol, "About Europol: Helping Make Europe Safer," May 20, 2025, https://www.europol.europa.eu/about-europol.

[25] Europol, "European Cybercrime Centre - EC3: Combating crime in a digital age," https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[26] Eurojust, "What we do," https://www.eurojust.europa.eu/about-us/what-we-do.

[27] These results do not distinguish the type of data that was encrypted (whether from devices or online services), nor do they identify the specific workarounds that were employed.

[28] Eurojust, "European Judicial Cybercrime Network," https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network.

[29] European Judicial Training Network, "About us," https://ejtn.eu/about-us/.

[30] Id.; European Judicial Training Network, "Exchanges," https://ejtn.eu/activity/exchanges/.

[31] European Union Agency for Law Enforcement Training, "The Agency," Apr. 5, 2023, https://www.cepol.europa.eu/about/the-agency.

[32] European Cybercrime Training and Education Group, "ECTEG," https://www.ecteg.eu/.

[33] Europol, "SIRIUS Project: Facilitating cross-border access to electronic evidence," Jan. 21, 2026, https://www.europol.europa.eu/how-we-work/sirius-project.

[34] e-Evidence Regulation, art. 3(8).

[35] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Official Journal of the European Union* L 130/1, May 1, 2014, art. 12(3),(4), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041 (hereinafter "European Investigation Order Directive").
As of this writing, the EIO is valid in every Member State, other than Denmark and Ireland.

[36] e-Evidence Regulation, art. 10(2)–(4); "Emergency case" is defined as a situation in which there is an imminent threat to the life, physical integrity or safety of a person, or to a critical infrastructure, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person. Id. art. 3(18).

[37] Id. art. 11(1).

[38] Id. art. 12 (laying out grounds for refusal); id. art. 15 (laying out penalties).

[39] Id. art. 3(9)–(12).

[40] Id. art. 4(1),(2).

[41] Id. art. 5(3),(4). Production orders can also be issued for the execution of a custodial sentence or detention order of at least four months, following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice. For Category Two, the sentence or detention order must be in connection with the smaller set of criminal offenses for which production orders can be issued.

[42] Id. art. 8.

[43] Id. art. 10(2)–(4). Grounds for objection are laid out in e-Evidence Regulation, art. 12. If data has been provided pursuant to an emergency request before an objection has been raised, the issuing state is required to either delete or restrict use of the data, depending on the nature of the objection. Id. art. 10(4).

[44] Id. art. 5(5)(i), art. 6(4)(g). *See also The EU Electronic Evidence Legislative Package: Sirius Annual Report*, Dec. 11, 2024, at 11–12 (describing procedural and substantive requirements for different data types), https://www.eurojust.europa.eu/sites/default/files/assets/files/sirius-e-evidence-legislative-package-annual-report.pdf.

[45] e-Evidence Directive, art. 3; id. art. 4(4) (requiring that the contact information for the designated establishment or representative is available and updated on the European Judicial Network's website).

[46] Id. art. 5.

[47] Id. art. 6.

[48] For updated information on the transposition status of the e-Evidence Directive, see European Union, "National transposition measures communicated by the Member States concerning Directive (EU) 2023/1544," EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32023L1544.

[49] European Commission, "Commission takes action to ensure complete and timely transposition of EU directives," Mar. 26, 2026, https://ec.europa.eu/commission/presscorner/detail/en/inf_26_679 (announcing that the Commission sent letters of formal notice for failing to communicate full transposition of the e-evidence Directive to Austria, Belgium, Bulgaria, Cyprus, Czechia, Estonia, Finland, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovenia, Spain, and Sweden). At the end of two months, the Commission can make formal requests to comply within a specified time period; failure to comply could result in referral to the Court of Justice of the European Union. See European Commission, "Infringement procedure," https://commission.europa.eu/law/application-eu-law/implementing-eu-law/infringement-procedure_en.

[50] Eurojust, *Eurojust meeting on the EU e-evidence package: Roles and responsibilities of Member States, service providers and Eurojust: Outcome report of the meeting of 30 September-1 October 2025*, Feb. 18, 2026, at 4, https://www.eurojust.europa.eu/sites/default/files/assets/files/eurojust-meeting-eu-e-evidence-package-2025.pdf.

[51] Houses of the Oireachtas, Criminal Justice (International Cooperation on Electronic Evidence and Other Matters) Bill 2026, https://www.oireachtas.ie/en/bills/bill/2026/59/

[52] Id.

[53] e-Evidence Regulation, art. 19(1).

[54] e-CODEX stands for "e-Justice Communication via Online Data Exchange" and is managed by eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. eu-LISA, "e-CODEX," https://www.eulisa.europa.eu/activities/large-scale-it-systems/e-codex.

[55] Commission Implementing Regulation (EU) 2025/1550 of 28 July 2025 establishing the technical specifications and other requirements for the decentralised IT system, referred to in Regulation (EU) 2023/1543 of the European Parliament and of the Council, *Official Journal of the European Union* L 2025/1550, July 29, 2025, annex, sec. 3.2, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202501550&qid=1756811646182 (noting the technical capacity constraints and directing that "electronic evidence shall be distributed through [the decentralized IT system] insofar as it does not exceed the threshold of 25 megabytes (25 600 kilobytes)") (hereinafter "Implementing Regulation").

[56] e-Evidence Regulation, art. 22.

[57] Implementing Regulation, recital 4 ("Member States may opt to use the reference implementation software developed by the Commission as their backend system in place of a national IT system. In order to ensure interoperability, both national IT systems and the reference implementation software should be subject to the same technical specifications and requirements set out in this Regulation."); id. annex, sec. 4 (laying out technical specifications).

[58] Implementing Regulation, annex, sec. 4.6; European Telecommunications Standards Institute, *Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers*, ETSI TS 104 144 V1.1.1, June 2025, https://www.etsi.org/deliver/etsi_TS/104100_104199/104144/01.01.01_60/ts_104144v010101p.pdf.

[59] Id. annex, sec. 8.

[60] e-Evidence Regulation, recital 84, art. 19(3).

[61] e-Evidence Regulation, art. 23.

[62] Id. art. 19(5).

[63] European Union Agency for Cybersecurity, *Advancing Software Security in the EU: The Role of the EU Cybersecurity Certification Framework*, Nov. 2019, at 4, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Advancing%20Software%20Security%20in%20the%20EU.pdf ("Security breaches are increasing in number and in severity. Quite often, the origin of security breaches is identified in omissions and errors that took place during software development or maintenance.").

[64] *See* Cloud Security Alliance CISO Community, *The "AI Vulnerability Storm": Building a "Mythos-Ready" Security Program*, Apr. 18, 2026, https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/04/mythosreadyv95.pdf; Europol, *The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026*, Publications Office of the European Union, 2026, https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf.

[65] e-Evidence Regulation, arts. 22, 23(1),(2).

[66] Implementing Regulation, annex, sec. 6.

[67] e-Evidence Regulation, art. 19(5).

[68] e-Evidence Regulation, art. 15(1).

[69] See 18 U.S.C. § 2702.

[70] e-Evidence Regulation, art. 17 (setting up a process by which a service provider can raise conflict of law concerns).

[71] CLOUD Act, supra note 23.

[72] 18 U.S.C. § 2523 (a)(2) (defining "United States person" as a citizen, national, or legal permanent resident of the United States, corporation incorporated in the United States, or unincorporated association with a substantial number of citizens or legal permanent residents of the United States); *see also* Jennifer Daskal, "Unpacking and Updating the CLOUD Act," *Lawfare*, Mar. 6, 2026, https://www.documentcloud.org/documents/27773001-unpacking-and-updating-the-cloud-act-daskal/; Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0," 71 *Stanford Law Review Online* 9, May 2018, https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/ (discussing the case and its broader implications).

[73] U.S. Department of Justice, Criminal Division, "Cloud Act Agreement Between the Governments of the U.S., United Kingdom of Great Britain and Northern Ireland," signed Oct. 3, 2019, https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern (including text of agreement and side letters); U.S. Department of Justice, Criminal Division, "Cloud Act Agreement Between the Governments of the U.S. and Australia," signed Dec. 15, 2021, https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia (including text of agreement and side letters).

[74] U.S. Department of Justice, Office of Public Affairs, "Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations," Mar. 2, 2023, https://www.justice.gov/archives/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations.

[75] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Union* L 119/1, May 4, 2016, art. 48, https://eur-lex.europa.eu/eli/reg/2016/679/oj. A U.S.-EU CLOUD Act Agreement could also address other issues — including by protecting against U.S. providers being subject to technical notices or other requirements that they redesign their systems to allow EU law enforcement access and thus minimizing broader geopolitical conflict. *See* Daskal, "The U.K.'s Decryption Order, the CLOUD Act, and Recommended Next Steps," *Lawfare*, July 21, 2025, https://www.lawfaremedia.org/article/the-u.k.-s-decryption-order--the-cloud-act--and-recommended-next-steps; Joseph Menn, "U.K. Orders Apple to Let It Spy on Users' Encrypted Accounts," *Washington Post*, Feb. 7, 2025, https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/.