



ELECTRONIC RECORDS

ELECTRONIC RECORDS (SB 1412)

EXECUTIVE SUMMARY

Senate Bill 1412 was enacted during the 2025 Regular Session of the General Assembly to address challenges faced by both criminal and civil stakeholders in obtaining out-of-state electronic records for use in Virginia proceedings. In addition to addressing these challenges, this bill also required the Crime Commission and the Joint Commission on Technology and Science to conduct a study related to Virginia's laws on electronic records. This study found that:

- Senate Bill 1412 addressed concerns with obtaining electronic records being stored out-of-state by businesses operating in Virginia;
- Electronic records can be stored anywhere in the world;
- Virginia has the same definition for “electronic record” as used in 48 other states;
- Virginia has enacted state law equivalents of certain federal statutes that allow the government to obtain out-of-state electronic records;
- Some companies have established portals for receiving requests for electronic records from law enforcement;
- Sharing electronic records with criminal defense counsel poses various challenges; and,
- Evolutions in technology, such as encrypted records and cryptocurrency, present challenges to obtaining electronic records.

Further study could be conducted on how to address evolving challenges, such as encrypted records and cryptocurrency.

BACKGROUND & METHODOLOGY

Senate Bill 1412 was enacted during the 2025 Regular Session of the General Assembly and took effect July 1, 2025.¹ The bill made the following changes to how out-of-state electronic records can be obtained for use in Virginia proceedings:

- **Criminal proceedings:** amended Virginia's search warrant statutes to explicitly authorize the issuance of search warrants for electronic records of any commercial enterprise transacting business in Virginia, regardless of where such records are stored.²
- **Civil proceedings:** added a provision in the Virginia Code that any foreign corporation transacting business in Virginia that has a registered agent in the Commonwealth is deemed to have consented to service of a subpoena.³

¹ Senate Bill 1412, 2025 Regular Session of the General Assembly (Sen. Ryan T. McDougle). <https://lis.virginia.gov/bill-details/20251/SB1412>.

² *Id.* The bill specifically amended Va. Code §§ 19.2-53 and 19.2-56 (2025).

³ *Id.* The bill specifically amended Va. Code § 8.01-301 (2025).

In addition, SB 1412 included an enactment clause that directed the Crime Commission and the Joint Commission on Technology and Science (JCOTS) to:

1. Review existing statutes on service of process and subpoenas related to electronic records; and,
2. Provide recommendations to update such statutes relating to the use of technology in the criminal justice system by November 15, 2025.⁴

Crime Commission and JCOTS staff worked in coordination to complete this study. Staff engaged in the following activities as part of the study:

- Identified federal and state statutes on electronic records;
- Reviewed federal and state case law relating to electronic records;
- Consulted with stakeholders to discuss the impact of SB 1412 and any potential issues related to electronic records and technology;⁵
- Met with representatives from companies offering electronic data storage services, including Amazon, Google, and Microsoft;
- Reviewed state statutes regulating cryptocurrency kiosks;⁶ and,
- Monitored discussions on blockchain technology and cryptocurrency from the JCOTS Blockchain Subcommittee.

STUDY FINDINGS

After reviewing the amendments to the Virginia Code made by SB 1412 and consulting with stakeholders, staff found that this legislation addressed the concerns of both criminal and civil stakeholders related to obtaining out-of-state electronic records from businesses operating in Virginia. For criminal stakeholders, the bill resolved an ambiguity in the Virginia Code as to whether search warrants can be issued by Virginia judicial officers for electronic records located outside of Virginia. Senate Bill 1412 resolved this ambiguity by amending Virginia Code §§ 19.2-53 and 19.2-56 to explicitly authorize the issuance of search warrants for electronic records of any commercial enterprise transacting business in Virginia, regardless of whether the electronic records are located in Virginia.⁷ The ambiguity arose because of the 2016 decision by U.S. Court of Appeals for the Second Circuit in *Microsoft Corp. v. United States*, where the court found that the federal district court lacked the authority to enforce a warrant compelling the production of electronic documents held outside the United States.⁸ The U.S. Supreme Court granted certiorari to review this *Microsoft* decision; however,

⁴ *Id.*

⁵ Staff met with the representatives from the Office of the Executive Secretary of the Supreme Court (which included representatives from Magistrate Services), the Policing Project at NYU School of Law, the Virginia Association of Commonwealth's Attorneys, the Virginia Indigent Defense Commission, and the Virginia Trial Lawyers Association.

⁶ A cryptocurrency kiosk or a Bitcoin ATM are similar to bank ATMs, except instead of providing cash from a bank account, they provide users with Bitcoin or some other cryptocurrency in exchange for cash. See "Bitcoin ATMs: how to use them and how do they work?" *Coinbase*, last viewed on Oct. 22, 2025, available at <https://www.coinbase.com/learn/tips-and-tutorials/bitcoin-atms-how-to-use-them-and-how-do-they-work>.

⁷ See *supra* note 1.

⁸ *Microsoft Corp. v. United States (In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation)*, 829 F.3d 197 (2nd Cir., July 14, 2016).

the issue in dispute became moot because the federal Clarifying Lawful Overseas Use of Data Act (CLOUD)⁹ was enacted before the U.S. Supreme Court could render a decision.¹⁰ Because the U.S. Supreme Court never ruled on the merits of the U.S. Court of Appeals decision in *Microsoft*, the reasoning set forth in that decision was being applied by some judicial officers in Virginia to deny the issuance of search warrants for electronic records stored outside of Virginia.

For civil stakeholders, the bill explicitly authorized the service of subpoenas on foreign corporations transacting business in Virginia.¹¹ The bill overturned the Virginia Supreme Court's 2015 decision in *Yelp v. Hadeed Carpet Cleaning*,¹² which held that Virginia courts were not authorized to enforce a non-party subpoena duces tecum against a foreign corporation.¹³ Furthermore, this amended language aligns the Virginia Code with the 2023 U.S. Supreme Court decision in *Mallory v. Norfolk Southern Ry.*, which found that an out-of-state corporation that has consented to in-state suits in order to do business in the forum is susceptible to suit there.¹⁴

Electronic records can be stored anywhere in the world.

Unlike physical records, electronic records can be stored anywhere in the world, or in multiple locations, and can be moved to another location in a matter of seconds. The location where these electronic records are stored is referred to as their data residency, or “the physical place where the data centers, servers or other systems that store or handle the data are located.”¹⁵ In consulting with representatives from Amazon Web Services, Google, and Microsoft, electronic records, especially records stored on cloud-computing services,¹⁶ do not tend to have fixed data residency, but instead can be moved across national or international borders.¹⁷ Additionally, with large storage companies like Amazon Web Services, Google, or Microsoft, there is no centralized database where all data is stored. Instead, data storage is based on a variety of factors, such as the needs of the customer and the type of data being stored.

⁹ The CLOUD Act was enacted into law under the Consolidated Appropriations Act of 2018. Consolidated Appropriations Act of 2018, H.R. 1625, 115th Cong. (2018) (Rep. Edward R. Royce). <https://www.congress.gov/bills/115th-congress/house-bill/1625>.

¹⁰ *United States v. Microsoft Corp.*, 584 U.S. 236 (Apr. 17, 2018). The CLOUD Act amended the Stored Communications Act (18 USC § 2701 et seq.), and the amendment authorized the issuance of warrants for electronic records held by companies operating in the United States regardless of the location of the electronic records.

¹¹ See *supra* note 1.

¹² *Yelp v. Hadeed Carpet Cleaning*, 289 Va. 426 (Va. Sup. Ct., Apr. 16, 2015).

¹³ *Yelp* at 437.

¹⁴ *Mallory v. Norfolk Southern Ry.*, 600 U.S. 122 (June 27, 2023).

¹⁵ Kosinski, Matthew. “Data sovereignty versus data residency: What’s the difference?” *IBM Think*. Last viewed Oct. 20, 2025, available at <https://www.ibm.com/think/topics/data-sovereignty-vs-data-residency>.

¹⁶ “Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale.” Microsoft. “What is cloud computing?” Last viewed on Oct. 20, 2025. Available at <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing#:~:text=Cloud%20computing%20defined,resources%2C%20and%20economies%20of%20scale>.

¹⁷ See *supra* note 14 (“As data moves through an organization's cloud-connected IT infrastructure, it can cross many borders.”).

Virginia has the same definition for “electronic record” as used in 48 other states.

Virginia, along with 48 other states, has enacted the Uniform Electronic Transactions Act, or UETA.¹⁸ This act, which has been adopted as part of the Virginia Code, defines “electronic record” as “...a record created, generated, sent, communicated, received, or stored by electronic means.”¹⁹ While the term “electronic record” is not explicitly defined in the Virginia Code search warrant statutes that were amended by SB 1412 (Va. Code §§ 19.2-53 & 19.2-56),²⁰ the Code cross-references the UETA definition in two other search warrant statutes (Va. Code §§ 19.2-54 & 19.2-56.2), as well as in a statute that describes the records of the circuit court clerks (Va. Code § 17.1-258.1). The Virginia Code also contains six additional definitions for “record” or “electronic record,”²¹ as well as two definitions for “electronic document,”²² which are similar to the definition in the UETA. The phrase “electronic record” could be defined in Virginia’s search warrant statutes (Va. Code §§ 19.2-53 & 19.2-56) to provide clarity and uniformity on what constitutes such a record.²³

Virginia has enacted state law equivalents of certain federal statutes that allow the government to obtain out-of-state electronic records.

Even before the passage of SB 1412, Virginia had enacted several statutes modeled after federal laws to allow the government to obtain out-of-state electronic records. The Stored Communications Act (SCA),²⁴ which provides the process by which the federal government can access the contents of electronic records held by remote computing or electronic communication services, is codified under Virginia Code § 19.2-70.3. Additionally, the Wiretap Act²⁵ and the Pen Register Act,²⁶ which generally provide the processes by which the federal government can track or intercept electronic communications, are codified under Virginia Code §§ 19.2-62 to 19.2-70 and Virginia Code §§ 19.2-70.1 and 19.2-70.2, respectively.

¹⁸ Uniform Law Commission. “Electronic Transactions Act.” Last viewed on Oct. 20, 2025. Available at

<https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034>. New York is the only state that has not enacted the UETA; however, the New York definition of “electronic record” is similar to what is used in the UETA. See New York State Technology Law § 302(2) (“‘Electronic record’ shall mean information, evidencing any act, transaction, occurrence, event, or other activity, produced or stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities.”).

¹⁹ Va. Code § 59.1-480(7) (2025).

²⁰ See *supra* note 1.

²¹ Va. Code §§ 8.1A-201(31) (“‘Record’ means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.”), 8.9-102(70) (“‘Record,’ except as used in ‘for record,’ ‘of record,’ ‘record or legal title,’ and ‘record owner,’ means information that is inscribed on a tangible medium or which is stored in an electronic or other medium and is retrievable in perceivable form.”), 13.1-603 (“‘Electronic record’ means information that is stored in an electronic or other nontangible medium and is retrievable in paper form through an automated process used in conventional commercial practice, unless otherwise authorized in accordance with subdivision A 10 of § 13.1-610.”), 13.1-803 (“‘Electronic record’ means information that is stored in an electronic or other medium and is retrievable in paper form through an automated process used in conventional commercial practice, unless otherwise authorized in accordance with subsection J of § 13.1-810.”), 42.1-77 (“‘Electronic record’ means a public record whose creation, storage, and access require the use of an automated system or device. Ownership of the hardware, software, or media used to create, store, or access the electronic record has no bearing on a determination of whether such record is a public record.”), and 64.1-116 (“‘Record’ means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.”).

²² Va. Code §§ 47.1-2 (“‘Electronic document’ means information that is created, generated, sent, communicated, received, or stored by electronic means.”) and 55.1-661 (“‘Electronic document’ means a document received by the clerk in electronic form.”).

²³ See Va. Code § 59.1-480(7) (2025) for the definition of electronic record in the UETA.

²⁴ 18 U.S.C. § 2701 *et seq.* (2025).

²⁵ 18 U.S.C. § 2510 *et seq.* (2025).

²⁶ 18 U.S.C. § 3121 *et seq.* (2025).

Some companies have established portals for receiving requests for electronic records from law enforcement.

Companies such as Amazon Web Services,²⁷ Google,²⁸ and Microsoft,²⁹ have created online portals through which law enforcement can submit requests for electronic records. Additionally, some companies publish reports on the number of law enforcement requests they receive and what kind of data they are providing to law enforcement.³⁰ However, it is not known how many companies offer such a portal, as practices can vary by company. Furthermore, it is unclear whether attorneys can use these portals to serve legal process, or if such process must be served by a separate means.³¹

Sharing electronics records with criminal defense counsel poses various challenges.

While law enforcement and Commonwealth's Attorneys informed staff that they generally do not experience issues receiving electronic records pursuant to a search warrant or court order, staff found that various challenges exist as it relates to the Commonwealth sharing electronic records with criminal defense counsel. Such challenges include needing specific programs to review electronic records, ensuring that defense counsel has access to the same data as the Commonwealth, and creating secure processes to protect sensitive information.³² The solutions to such challenges may vary on a case-by-case basis, as programs needed to review electronic records vary by company and the sensitivity of the data and protections needed will depend on the nature of the records.

Evolutions in technology, such as encrypted records and cryptocurrency, present challenges to obtaining electronic records.

Staff discovered that some companies are encrypting electronic records in a manner such that the company itself cannot view the contents. For example, some messaging apps, such as Telegram, encrypt messages sent using the app so that only the sender and recipient can see the contents of the messages.³³ Hence, if law enforcement sends a search warrant to a company like Telegram that

²⁷ Law Enforcement Request Tracker, *Amazon*, last viewed on Oct. 21, 2025, available at <https://ler.amazon.com/us>.

²⁸ Law Enforcement Request System, *Google*, last viewed on Oct. 21, 2025, available at https://lers.google.com/signup_v2/landing.

²⁹ Law Enforcement Request Portal, *Microsoft*, last viewed on Oct. 21, 2025, available at <https://leportal.microsoft.com/home>.

³⁰ See e.g., Law Enforcement Information Requests, *Amazon*, last viewed on Oct. 21, 2025, available at <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEE>; Government Requests for Customer Data Report, *Microsoft*, last viewed on Oct. 21, 2025, available at <https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data>. See also Transparency Report, *AT&T*, last viewed on Oct. 22, 2025, available at <https://sustainability.att.com/reports/transparency-report>.

³¹ See Serving Requests for User Data on Behalf of Defendants in Criminal Proceedings in the U.S. on Google, *Google Help*, last viewed on Oct. 21, 2025, available at https://support.google.com/faqs/answer/7269563?hl=en&ref_topic=6151009&sjid=11137679729649503564-NA (directs attorneys in criminal cases to serve legal processes on Google's registered service agent, the Corporation Service Company); but see Welcome to VSAT Intake, *Verizon*, last viewed on Oct. 21, 2025, available at <https://legalintake.verizon.com/> (Verizon's online portal allows "[a]uthorized government agencies, law enforcement, and law firms" to "submit legal process").

³² Staff was made aware of these issues when meeting with representatives from the Virginia Indigent Defense Commission on May 21, 2025.

³³ Telegram Privacy Policy, *Telegram*, last viewed on Oct. 22, 2025, available at <https://telegram.org/privacy?setln=uz#9-your-rights-regarding-the-personal-data-you-provide-to-us> ("4.2. End-to-End Encrypted Data[.] Your messages, media and files from secret chats ..., as well as the contents of your calls and the data you store in your Telegram Passport are processed only on your device and on the device of your recipient. Before this data reaches our servers, it is encrypted with a key known only to you and the recipient. While Telegram servers will handle this end-to-end encrypted data to deliver it to the recipient – or store it in the case of Telegram Passport data, we have no ways of deciphering the actual information. In this case, we neither store nor process your personal data, rather we store and process random sequences of symbols that have no meaning without the keys which we don't have.")

encrypts electronic records in such a manner, the company will be unable to provide the electronic records due to the encryption.³⁴ Federal Rule of Criminal Procedure 41(b)(6)³⁵ was adopted at the federal level to allow law enforcement to use remote access to obtain these records; however, this process differs from a traditional search warrant, as a search warrant issued under this rule authorizes the copying of information directly from a device, instead of obtaining the information through a company or other record holder. However, even with this Rule 41 authorization, accessing a device itself to obtain encrypted data can be difficult.³⁶

Finally, staff identified concerns related to the growing use of blockchain.³⁷ These concerns specifically focus on cryptocurrency, which is a digital currency purchased and sold using a blockchain,³⁸ that can be used in various fraudulent and ransomware schemes. The scope of the fraud can be significant; “Americans, often retirees, lost around \$240 million to crypto ATM³⁹ scams in the first six months of this year, according to the FBI.”⁴⁰ Most states have introduced or have pending legislation regarding cryptocurrency, and at least 16 states have enacted legislation regulating some aspect of cryptocurrency.⁴¹ However, state regulation of cryptocurrency is a much broader measure that extends beyond access to electronic records.

CONCLUSION

Senate Bill 1412 addressed the concerns of criminal and civil stakeholders in regard to obtaining out-of-state electronic records for use in Virginia proceedings.⁴² Electronic records can be stored anywhere in the world. Virginia has adopted a definition of “electronic record” that is identical to 48 other states, and has enacted various statutes that are consistent with federal laws to allow government access to

³⁴ See *e.g. Id.* (“8.3. Law Enforcement Authorities[.] If Telegram receives a valid order from the relevant judicial authorities that confirms you're a suspect in a case involving criminal activities that violate the Telegram Terms of Service, we will perform a legal analysis of the request and may disclose your IP address and phone number to the relevant authorities. If any data is shared, we will include such occurrences in a quarterly transparency report published at: <https://t.me/transparency>.”)

³⁵ Fed. R. Crim. P. 41(b)(6) (2025).

³⁶ See Finklea, Kristin (Jan. 6, 2025). “Law Enforcement and Technology: The ‘Lawful Access’ Debate.” *Congress.Gov*, available at <https://www.congress.gov/crs-product/IF11769> (“With respect to devices, access to devices and the content on them may be locked and encrypted. Various factors can affect law enforcement's efforts to gain access to a device and its contents. For instance, law enforcement attempting to unlock a device with brute force would likely use software to try every possible combination of keys in an attempt to unlock the device. The success of this method may depend, among other things, on the amount of time available to try and unlock a device, device limits on passcode attempts, and the number of keys used in the passcode.”)

³⁷ A blockchain is “a decentralized, immutable, and public ledger.” Dr. Haj Hasan, Waleed Y.W. (May 7, 2025). “Innovative Disruption: State-Specific Considerations for Cryptocurrencies and Blockchain Technology.” *Presentation for Virginia's Joint Commission on Technology and Science, Blockchain Subcommittee*, slide 2, available at https://studiesvirginiageneralassembly.s3.amazonaws.com/meeting_docs/documents/000/002/592/original/Blockchain_MeetingMaterials.pdf?1746713796.

³⁸ See Peterson, Nathan (May 6, 2025). “What is Cryptocurrency and How Does It Work?” *Charles Schwab*, available at <https://www.schwab.com/learn/story/cryptocurrencies-what-are-they>.

³⁹ See *supra* note 6.

⁴⁰ Devine, Curt; Kamp, Majlie de Puy; Abou-Ghazala, Yahya; Tolan, Casey; Lah, Kyung; O’Kruk, Amy; Manley, Byron; and Stubbs, Eleanor (Oct. 14, 2025). “Crypto crime scene: How the companies behind crypto ATMs profit as Americans lose millions to scams.” *CNN*, available at <https://www.cnn.com/interactive/2025/10/us/crypto-atm-scams-companies-profit-invs-vis/>.

⁴¹ See “Cryptocurrency, Digital or Virtual Currency and Digital Assets 2025 Legislation.” *NCSL*, updated Sept. 11, 2025, available at <https://www.ncsl.org/financial-services/cryptocurrency-digital-or-virtual-currency-and-digital-assets-2025-legislation> (as of September 11, 2025, Arizona, Arkansas, Connecticut, Georgia, Iowa, Kentucky, Maryland, Montana, Nebraska, North Dakota, Oregon, South Dakota, Utah, Vermont, Washington, and Wyoming have enacted legislation regulating some aspect of cryptocurrency).

⁴² See *supra* note 1.

electronic records. Some companies have created online portals for law enforcement to request electronic records; however, it is unknown how many of these portals exist and what processes companies have in place for attorneys to serve other legal process.

Further study could be conducted on how to address evolving challenges, such as encrypted records and cryptocurrency.

ACKNOWLEDGEMENTS

The Crime Commission and the Joint Commission on Technology and Science wish to thank the following for their assistance with this study:

Amazon Web Services

Google

Microsoft

Office of the Executive Secretary of the Supreme Court

Virginia Association of Commonwealth's Attorneys

Virginia Commonwealth's Attorneys' Services Council

Virginia Indigent Defense Commission

Virginia Judicial System – Magistrate Services

Virginia Trial Lawyers Association