CLOUD STORAGE & LAW ENFORCEMENT

CHALLENGES IN OBTAINING DATA STORED ON THE CLOUD

Overview

In the age of digital evidence, law enforcement personnel are encountering cloud-based data in criminal investigations at unprecedented frequencies. In a cloud storage model, data is saved to a service provider's remote storage locations instead of the user's local storage devices (e.g., hard drives, thumb drives, compact discs).[i] The emergence of the cloud has presented unique challenges to many actors across the criminal justice system. The purpose of this guide is to discuss the inherent challenges of obtaining data stored on cloud-based platforms, followed by resources for navigating them.

Challenges in Accessing Cloud-based Data

- **Infrastructure**: Basic components of the cloud's infrastructure make obtaining data a daunting task. Because the data is stored remotely, law enforcement cannot simply obtain a search warrant and seize a suspect's computer to access the digital evidence. It is also impractical and infeasible for law enforcement to seize servers from data centers without infringing on the privacy rights of other clients, as cloud servers house files from multiple users.[ii] Additionally, servers are often located in different jurisdictions than that of the investigating agency. Search warrants and subpoenas may not be honored by the jurisdiction housing the server, especially when servers are housed overseas.[iii]
- **Legal Considerations**: Although there is no government statute specifically addressing cloud storage, such cases fall under the purview of Title II of the Electronic Communication Privacy Act of 1986 (ECPA), also known as the Stored Communications Act (SCA). Because the ECPA was codified long before the proliferation of cloud storage or web-based email services, many law enforcement professionals and privacy advocates feel that the law is not suited to address the needs of the current technological climate.[iv] For example, under the ECPA, law enforcement does not need a warrant for stored communications that are more than 180 days old. Privacy advocates argue that with changes in technology that allow for immense data storage, communications older than 180 days should be protected from warrantless searches under the Fourth Amendment.[v] As legislative reform continues to be proposed, law enforcement must keep abreast about the potential changes to the statue as they develop.[vi] Additionally, the ECPA does not regulate how long service providers must retain user data, so data retention practices can vary greatly among service providers. If user records no longer exist, law enforcement cannot access the data, even with a subpoena or search warrant.[vii]
- **Internet Service Providers (ISPs)** Investigators are reliant on ISPs for obtaining digital evidence stored in the cloud. The employee of the cloud provider, however, may not hold forensic investigator credentials, thus leading to potential legitimacy concerns in court. The introduction of a third party in the chain of custody may influence the integrity of the digital evidence. To preserve the trustworthiness of evidence, investigators should ensure that the chain of custody clearly depicts how the digital data was collected, analyzed, and stored. [viii]

Resources

SEARCH, The National Consortium for Justice Information and Statistics, offers several resources to criminal justice partners for obtaining cloud-based data. The following tools are accessible through their website, www.search.org.[ix]

- **Internet Service Provider List**: The ISP List is a database of Internet service and other online content providers that assists investigators in obtaining data needed for a case. For each Internet Service Provider, there is a listing of legal contact information and instructions needed to serve subpoenas, court orders, and search warrants.
- **Quick Access ISP Information**: Through a simple online request form, SEARCH provides law enforcement investigators with documents to aid in data requests to ISPs. These files include legal process policies and law enforcement compliance guides for popular companies, such as Apple, Snapchat, and Uber.

The National White-Collar Crime Center (NW3C) also provides support services to assist law enforcement agencies in obtaining cloud-based data. NW3C offers online and classroom training courses, such as, *Identifying and Seizing Electronic Evidence, Searching without a Warrant,* and *The Stored Communications Act.*

CYBER SECURITY CONSIDERATIONS FOR POLICE DATA IN THE CLOUD

Overview

With the emergence of body worn cameras, cellphone multimedia, and social media, many law enforcement agencies are opting for cloud-based platforms to manage and store the large volume of digital data generated by these technologies.[x] The purpose of this section is to discuss considerations for protecting police data stored in the cloud, followed by resources for implementing and maintaining cloud-based solutions.

Considerations

- **Threats:** Law enforcement agencies utilizing cloud-based platforms for storage solutions are susceptible to cybersecurity threats, such as data breaches, unauthorized access, and loss of data. One of the most common threats to cloud-stored data is ransomware, a type of malware that inhibits access to systems or data. In a ransomware attack, "the malicious cyber actor holds systems or data hostage until the ransom is paid. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted."[xi] Although many police agencies rely on third-party vendors to create a secure environment, the owner of the data is ultimately responsible for ensuring protection.[xii] Police officials can mitigate potential threats by choosing a cloud service provider that adheres to the security standards outlined by the FBI's Criminal Justice Information Services (CJIS) Security Policy.[xiii]
- **Data Ownership:** When using third-party vendors to manage and store data, questions over ownership may arise. The law enforcement agency should be the owner of the data and ensure that this is represented in the contract. The department should also be familiar with the procedure for transferring data to another server in the event that the agency ends the contract with the vendor.[xiv]
- **Security Compliance**: The FBI mandates that cloud solutions must comply with security regulations set by Criminal Justice Information Services (CJIS) to obtain data from state and federal databases. Cloud providers should be vigilant in maintaining compliance, as some digital records may be subject to multiple security standards.[xv] For example, video from a body-worn camera may become evidence for a criminal case (CJIS compliance), recorded in a medical facility (HIPAA compliance), and include information about an individual's employment or income (IRS 1075 compliance).[xvi]

Resources

- **Cloud Technology Primer:** The Bureau of Justice Assistance's *Public Safety Primer on Cloud Technology* provides public safety agencies with introductory guidance on cloud technology, services provided by the cloud, and considerations for contracts with cloud vendors. The resource also contains a glossary of terms and definitions regarding the cloud, followed by recommended readings for government leaders wanting to learn more about cloud technology.[xvii]
- **Implementation Guides**: The IACP's *Guiding Principles on Cloud Computing in Law Enforcement* is a comprehensive guide providing law enforcement agencies with key considerations for implementing cloud computing services. The report offers information on cost, operability, security, and vendor contracts.[xviii] Additional guidance for CJIS compliance can be found in the FBI's *Recommendations for Implementing Cloud Based Solutions*. [xix] This report provides recommended policies and procedures for police agencies implementing cloud computing solutions.

---

[i] Rouse, M. (2016, May). What is cloud storage? Retrieve from http://searchstorage.techtarget.com/definition/cloud-storage

[ii] Zawoad, S., & Hasan, R. (2013). *Digital Forensics in the Cloud*. CrossTalk. The Journal of Defense Software Engineering, 26(5), 17–20.29

[iii] Grispos, G., Storer, T., & Glisson, W. B. (2012). *Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics*. International Journal of Digital Crime and Forensics, Volume 4, Issue 2, Pages 28-48

[iv] Center for Democracy & Technology. (2015, May 13). Electronic Communications Privacy Act Primer. Retrieved from https://cdt.org/insight/electronic-communications-privacy-act-primer/

[v] American Civil Liberties Union, "Modernizing the Electronic Communications Privacy Act (ECPA). Retrieved from https://www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa

[vi] Introduced bills and active legislation can be found at www.congress.gov

[vii] *Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence*. (2015). IACP Summit Report. Retrieved from http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf

[viii] Zawoad, S., & Hasan, R. (2013). *Digital Forensics in the Cloud*. CrossTalk. The Journal of Defense Software Engineering, 26(5), 17–20.29

[ix] Resources. (2017). Retrieved August 23, 2017, from http://www.search.org/

[x] Global Justice Information Sharing Initiative. (2016). *Public Safety Primer on Cloud Technology* (United States, Department of Justice, Bureau of Justice Assistance).

[xi] Department of Homeland Security, US-CERT. (2016, July 11). *Ransomware: What It Is and What to Do about It*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

[xii] Wyllie, D. (2017, June 22). *How to Protect Your Digital Video Evidence from a Cyberattack*. Retrieved from https://www.policeone.com/policing-in-the-video-age/articles/375309006-How-to-protect-your-digital-video-evidence-from-a-cyberattack/

[xiii] Federal Bureau of Investigation, Criminal Justice Information Services Division. (2017, June 5). Criminal Justice Information Services (CJIS) Security Policy. Retrieved from https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

[xiv] Griffith, D. (2016, October 10). *The Cloud: Beyond Data Storage*. Retrieved from http://www.policemag.com/channel/technology/articles/2016/10/the-cloud-beyond-data-storage.aspx

[xv] Global Justice Information Sharing Initiative.

[xvi] Ibid.

[xvii] Ibid.

[xviii] *Guiding Principles on Cloud Computing in Law Enforcement*. (2015). Retrieved August 28, 2017, from http://www.theiacp.org/Portals/0/documents/pdfs/CloudComputingPrinciples.pdf

[xix] United States, Department of Justice, Federal Bureau of Investigation. (2012). *Recommendations for Implementing Cloud Based Solutions*. Clarksburg, WV.