exterro

Addressing the Proposed

NC Ethics Opinions

CLOUD COMPUTING IN THE LEGAL SPACE

By Sarah Brown

ADDRESSING THE PROPOSED NC ETHICS OPINIONS

CLOUD COMPUTING IN THE LEGAL SPACE

For attorneys and law firms considering using a cloud-based legal solution, a specific ethics decision from a state bar association has been a long time coming.

North Carolina tackled legal SaaS head-on when it issued "Proposed 2010 Formal Ethics Opinion 7: Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property."

In the document, the drafters of the proposed ethics decision pose the following questions, which all attorneys should be able to answer before choosing a SaaS vendor. Exterro has taken the liberty of providing answers to these questions even before they are asked by the marketplace:

Q: What is the history of the SaaS Vendor?

A: Exterro has been building, deploying and implementing robust legal technology solutions since 2004. With enterprise, hosted and cloud-based legal solutions, Exterro is entirely dedicated to producing legal software that meets uniquely legal needs.

Q: How is it stable financially?

A: We have been consistently financially stable since 2004 and our trajectory is that of growth.

Q: Has the lawyer read the user or license agreement terms, including the security policy, and does he/she understand the meaning of the terms?

A: Exterro provides each end user with a copy of its license agreement terms and security policy after an NDA is in place. Additionally, it provides quick-start guides, glossaries, and online help to ensure each client company constituent fully understands his or her obligations with regards to privacy and data security.

Q: Does the SaaS vendor's Terms of Service or Service Level Agreement address confidentiality?

A: Exterro clients' terms of service and service level agreements protect clients' confidentiality, security and privacy according to SAS 70 Type II process standards, including change management software, access controls, and privacy processes. Additionally, Exterro provides firewalls and private VPN tunnels, provides intrusion detection and monitoring tools for a second line of defense. Any additional privacy concerns or processes unique to a particular client are addressed and specified contractually.

Q: If not, would the vendor be willing to sign a confidentiality agreement in keeping with the lawyer's professional responsibilities?

A: Yes. In addition to the confidentiality clause in the SLA, Exterro is always willing to provide an extra level of assurance by signing confidentiality agreements with its clients.

Q: Would the vendor be willing to include a provision in that agreement stating that the employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect client information?

A: The hosting facilities and data centers that Exterro uses for its cloud product have a fiduciary responsibility to Exterro and act as agents on behalf of Exterro and its clients, and by extension to its clients.

Q: How does the SaaS vendor, or any third party data hosting company, safeguard the physical and electronic security and confidentiality of stored data?

A: SAS 70 Type II compliance ensures that all data is both physically and electronically secure and confidential, including a secure infrastructure and audited processes for handling data breaches. We secure data at rest and in transit through encryption and change control management and monitoring processes and software.

Q: Has there been an evaluation of the vendor's security measures including the following: firewalls, encryption techniques, socket security features, and intrusion-detection systems?

A: Yes. The solution and its servers are SAS 70 Type II compliant. We partner with our client companies to ensure data remains secure, and our cloud product guarantees, through SLAs and other means, secure information at rest and additional hosting options for security in transit, including encryption in transit and/or private VPN tunnels, as well as firewalls and regular intrusion and data breach detection.

Q: Has the lawyer requested copies of the SaaS vendor's security audits?

A: Clients and prospects may see an electronic or hard copy of Exterro's security audits with a signed NDA.

Q: Where is data hosted? Is it in a country with less rigorous protections against unlawful search and seizure?

A: All Exterro's clients' data is hosted in the United States on SAS 70 Type II compliant servers that are geographically dispersed for disaster recovery purposes.

Q: Who has access to the data besides the lawyer?

A: We limit access to data according to strict SAS 70 Type II Standards, including strict internal access and maintenance controls. All access is tracked through change management and audit trails. Who All access is approved by the customer, known and tracked.

Q: If the lawyer terminates use of the SaaS product, or the service otherwise has a break in continuity, how does the lawyer retrieve the data and what happens to the data hosted by the service provider?

A: Exterro offers expert services to provide a rigorous training and implementation program that ensure users fully understand how to get data into and out of the system securely. We also provide a fully validated exit strategy for each cloud client, as well as a simple and secure means for pulling data "offline." The client firm would retrieve the data via an industry standard format, including CSV. Data is stored in a non-proprietary format so the customer can choose delivery method. The data hosted by Exterro goes through standard data retention processes as determined by SAS 70 and any customer-defined limitations, such as disposition and retention periods, determined at contractual inception.

Q: If the SaaS vendor goes out of business, will the lawyer have access to the data and the software or source code?

A: Access to data and software is guaranteed contractually according to SAS 70 Type II standards.

Q: Can the lawyer get data "off" the servers for the lawyer's own offline use/backup?

A: Yes. Through CSV or Excel export and dynamic, rich reporting capabilities, users with correct access controls and privacy clearance can export any needed data in order to work offline or serve as a paper backup.

Q: If the lawyer decides to cancel the subscription to SaaS, will the lawyer get the data?

A: Yes. Exterro offers expert services to provide a rigorous training and implementation program that ensure users fully understand how to get data into and out of the system securely. We also provide a fully validated exit strategy for each cloud client, as well as a simple and secure means for pulling data "offline." The client firm would retrieve the data via an industry standard format, including CSV. Data is stored in a non-proprietary format so the customer can choose delivery method.

Q: Is data supplied in a non-proprietary format that is compatible with other software?

A: Exterro stores all data in industry-standard, non-proprietary formats. This ensures easy integrations as well as data migrations where necessary.

Sarah Brown is the Corporate Communications Manager at Exterro, Inc., a leading provider of legal and e-discovery workflow management software solutions. She is a board member of the Legal Governance, Risk and Compliance Center for Innovation, an active member of Women in E-Discovery, and brings her broad knowledge of industry trends to her role directing corporate and product messaging, media relations and marketing at Exterro, Inc.

CONNECT WITH US

EXTERRO.COM: info@exterro.com

Phone: **1-877-EXTERRO (398-3776)**
Fax: **(800) 408-7310**

Twitter: **www.twitter.com/exterro**
LinkedIn: **http://tinyurl.com/exterrofusion.com**
Facebook: **http://tinyurl.com/exterro**