Cybersecurity and Arbitration: Protecting Your Documents and Ensuring Confidentiality

By Tankut Eker, Dan Meyers and Al-Karim Makhani

One of the core advantages that drives parties to arbitrate is the promise of confidentiality. Unlike court proceedings, which are open to the public, arbitrations provide parties with a private forum through which to air and resolve their disputes. This advantage, however, is threatened by unwanted and unauthorized intrusions by cybercriminals, who have become ubiquitous in the modern world and target the legal sector with particular vigilance. Notwithstanding this modern threat, most arbitration practitioners continue to rely upon unsecure platforms to store, serve, and file their documents, most notably unencrypted emails and commercially available "cloud" repositories.

Particular care should be paid in international arbitrations, where the parties, counsel, and arbitrators frequently hail from different countries (or continents), triggering a web of data privacy laws that affirmatively obligate parties to take reasonable security measures to protect sensitive and personal information. Combined with attorney ethical obligations to ensure the confidentiality of client information, this intersection of regulatory requirements and security shortcomings creates a perfect storm for practitioners and their clients alike.

"Earlier this year, the FBI's Cyber Division issued Alert 160304-1, which specifically warned that cybercriminals are actively targeting the legal sector to obtain non-public information about corporations in order to turn potentially significant profits on stock markets trades."

Fortunately, the current circumstances are not all doom-and-gloom. The legal technology sector has developed convenient and secure platforms that empower parties, their counsel and the arbitrators themselves to not only store, serve, and file documents securely, but also to collaboratively draft documents from opposite ends of the world.

Confidentiality vs. Hackers

Practitioners are well-versed in the benefits of arbitration over other avenues of dispute resolution. Since the inception of arbitration centuries ago, one key component remains unchanged in its significance—confidentiality. In his 1934 work, *The Historical Background of Commercial Arbitration*, Wolaver suggests that the origins of arbitration lay in the settlement of trade disputes by amicable *private* tribunals.[1] Now, more than ever, confidentiality is a vital component to the process. A survey of U.S. and European users of international commercial arbitration conducted on behalf of the London Court of International Arbitration by the London Business School listed confidentiality as the most important benefit.[2] Arbitrations are held in private and a party's involvement in arbitration proceedings is confidential. This is in stark contrast to most domestic legal systems, where court hearings are open to the public, the identity of the parties is a matter of public record, and most filings can be accessed by any interested third party.

"Although there have been recent attempts to make email more secure through encryption or creating a private wire between senders and receivers, these options remain infrequently used."

The recently reported cyberattacks on law firms such as Mossack Fonseca, Cravath Swaine & Moore, and Weil Gotshal & Manges have put the issue of law firm cybersecurity in the spotlight. But the truth is that such attacks are neither new nor infrequent. Cyberattacks against law firms have been on the rise for a number of years—unsurprising given the wealth of highly sensitive and valuable client information that law firms possess. It is a misconception that these attacks are randomly carried out by bored, tech-savvy teenagers looking for a buzz. They are often conducted by sophisticated, well-funded hackers looking for specific information about pending deals or disputes. Earlier this year, the FBI's Cyber Division issued Alert 160304-1, which specifically warned that cybercriminals are actively targeting the legal sector to obtain non-public information about corporations in order to turn potentially significant profits on stock markets trades.[3]

Basic Email Is Not Secure

Email is the most popular form of communication (along with texting) in the world. But it is also one of the most vulnerable to hacking, which can take the form of viruses, malware, trojans, keyloggers, man-in-the-middle, and man-in-the-browser attacks (not to mention potential breaches of devices, networks, and servers themselves). Even Yahoo's own Safety Center advises, "Never send your credit card number, Social Security number, bank account number, driver's license number or similar details in an email, which is generally not secure. Think of email

as a paper postcard—people can see what's written on it if they try hard enough."[4]

To understand why email is not secure, one must remember that the historical design of the same fundamental email system that we use today was never conceived with security in mind. To the contrary, when email was originated decades ago internet usage was extremely limited and everything that was transferred was done openly and could be accessed and read by everyone else "online." Of course, significant advances have occurred in privacy and security in the intervening years—foremost of which being passwords, which are designed to limit access to emails to the intended recipients.

But the fact remains that every email resides in many locations at once. The sender's device (smart phone, tablet, computer) is the originating source, but before the email arrives at the recipient's device, the email will travel through myriad intermediary networks, servers, routers, and switches which are often operated by different providers. Each of these locations is a separate vulnerability point to unauthorized intrusions. A hacker that infiltrates any of these locations can access (and even alter) the content of the emails that are passing through.

Although there have been recent attempts to make email more secure through encryption or creating a private wire between senders and receivers, these options remain infrequently used.

Most Cloud Repositories Are Not Secure

The alternative methods that many arbitrators, practitioners and counsel rely upon to store, transmit, serve, and "file" sensitive documents in an arbitration are commercially available "cloud" repositories like Box, Dropbox, and similar platforms. But as with email, these environments were not designed with security as the priority and the results have been significant unauthorized intrusions, such as the 68 million Dropbox users that reportedly had their information hacked.[5]

"Because such platforms are designed from the start with an emphasis on security, the features that ensure confidentiality are multifaceted and nearly impossible to circumvent."

The Committee on Professional Ethics of the New York State Bar Association itself recognized the inherent problem of security in cloud environments when it issued Opinion 842, which concludes that a lawyer may only "use an online data storage system to store and back up client confidential information" if the lawyer first "takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under rule 1.6" and "exercise[s] reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential information of a client."[6]

"In today's digital age, attorneys and their clients can never be too careful when handling sensitive information contained in electronic documents."

While the various vulnerabilities of commercially available online storage environments are too many to discuss in-full, some of the highlights are:

- many such platforms claim ownership over all information that is uploaded, thus claiming the right to use and share such information for any disclosed purpose;
- the administrators and developers of such platforms have full access to the information shared;
- the security measures utilized by most platforms are not disclosed to users;
- users are typically not allowed to perform encryption on their own information before uploading;
- many providers utilize U.S.-based servers and are subject to U.S.-government eavesdropping programs (even if the users reside outside of the U.S.); and
- most of these solutions do not have built-in password protection or encryption for individual documents.

LegalTech to the Rescue

Fortunately for arbitrators, practitioners, and their clients, the gap between current (unsecure) practices and the need for confidentiality is being filled by the legal technology industry. Platforms such as TransCEND, which is specifically designed for the legal industry, empower arbitrators, parties, and their counsel to securely store, transmit, and edit sensitive documents from anywhere in the world.

Because such platforms are designed from the start with an emphasis on security, the features that ensure confidentiality are multifaceted and nearly impossible to circumvent. Security begins with multi-factor authentication to access the database in the first place (i.e., two sets of login criteria to obtain access). Thereafter, every file uploaded is encapsulated within an encryption shield to prevent the interception of data and the unauthorized extraction or distribution of content. Further, through

the use of access controls within the platform (known as "Information Rights Management"), the party uploading a document can control how much access they give to his or her counterparties (or to the arbitrators themselves). For example, when filing particularly sensitive documents through the platform, the receiving parties' access can be restricted to being able to view the contents through the platform while disabling the ability to edit, print, download or email the document to others. Even the ability to take a "screenshot" can be disabled.

Conclusion

In today's digital age, attorneys, and their clients can never be too careful when handling sensitive information contained in electronic documents. For the arbitration community—and in particular the international arbitration community—this means taking advantage of the technological advances that ensure the ability to share and collaborate without running afoul of your client's confidence and the web of regulatory security requirements.

Endnotes

1. *See* The Historical Background of Commercial Arbitration, available at http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=8693&context=penn_law_review.
2. *See* Bagner, "Confidentiality—A Fundamental Principle in International, Commercial Arbitration?" (2001) 18 Journal of International Arbitration 2.
3. *See* FBI's Cyber Division issued Alert 160304-1, available at https://info.publicintelligence.net/FBI-InsiderTradingHacking.pdf.
4. *See* https://safety.yahoo.com/Security/PREVENT-ID-THEFT.html
5. *See* https://www.washingtonpost.com/news/the-switch/wp/2016/09/07/hacked-dropbox-data-of-68-million-users-is-now-or-sale-on-the-dark-web/.
6. NYSBA Comm. on Professional Ethics of, Formal Op. 842 (2010).

Tankut Eker is the Managing Director of TransCEND, a secure document storage and collaboration platform frequently used in arbitrations. Dan Meyers is the President of the Consulting and Information Governance divisions at TransPerfect Legal Solutions (TLS) and a former litigation Partner at Bracewell & Giuliani LLP. Al-Karim Makhani is a Senior Case Consultant at TLS and a former Senior Associate in the Disputes group at Stephenson Harwood LLP.