White Paper

THE PERILS OF FILING CONFIDENTIALINFORMATION IN THE CYBER AGE

WIKILOCKS SECURITY MAKES IT POSSIBLE TO ADHERE TO ABA ETHICAL STANDARDS FOR CLIENT DATA PROTECTION

WikiLocks™

Powered By: WindTalker

ATTORNEYS HAVE A SACROSANCT ETHICAL OBLIGATION TO PROTECT CLIENT CONFIDENTIAL INFORMATION

The American Bar Association (ABA) is the leading ethical voice for American lawyers. In the May 2015 report: "American Bar Association Section of Labor & Employment — Law Ethics and Cybersecurity: Obligations to Protect Client Data" the following passage describes an attorney's obligations:

"Ethics rules, both from the ABA and in California, impose duties on attorneys to protect client confidences. They also require attorneys to practice competently and to supervise office staff and third parties with access to client data. The operation of these rules will require attorneys and law firms to implement reasonable information security practices to protect the confidentiality, integrity, and availability of client data. The failure to protect client data may lead to attorney discipline or malpractice liability."

LAWYERS, LIKE BUSINESSES, HAVE A LEGAL DUTY TO PROTECT PRIVACY

Businesses throughout the world have a legal duty to protect consumer privacy, and when this information is given to an attorney, the attorney also has an obligation to protect it. Here's the Wikipedia version on information that must be kept private:

"Information privacy or data protection laws prohibit the disclosure or misuse of information about private individuals. Over 80 countries and independent territories, including nearly every country in Europe and many in Latin America and the Caribbean, Asia, and Africa, have now adopted comprehensive data protection laws. The United States is notable for not having adopted a comprehensive information privacy law, but rather having adopted limited sectoral laws in some areas."

These laws are based on Fair Information Practice that was first developed in the United States in the 1970s by the Department for Health, Education and Welfare (HEW). The basic principles of data protection are:

- For all data collected there should be a stated purpose.
- Information collected by an individual cannot be disclosed to other organizations or individuals unless specifically authorized by law or by consent of the individual.
- Records kept on an individual should be accurate and up to date.
- There should be mechanisms for individuals to review data about them, to ensure accuracy. This may include periodic reporting.
- Data should be deleted when it is no longer needed for the stated purpose.
- Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited.
- Some data is too sensitive to be collected, unless there are extreme circumstances (e.g., sexual orientation, religion.)"[1]

[1] americanbar.org/content/dam/aba/multimedia/cle/materials/2016/04/ce1604lpi.authcheckdam.pdf

LEGAL FILINGS ARE GENERALLY OPEN TO THE PUBLIC AND ACCESSIBLE TO ALL

Because an open court system is deemed essential to a free democratic society, affording accountability, fostering public confidence, and providing notice of the legal consequences of behaviors and choices, unless filed under seal all legal filings and most court proceedings are entirely open to the public.

Anyone can go there or access them and the information can be published to the world via private blog or Facebook or Twitter or headlines in the New York Times or any medium whatsoever. However, there are good reasons for courts to keep parts of some proceedings confidential, such as confidential classified information, ongoing investigations, trade secrets, and the identities of minors, and this they will do.

The public in general and news media in particular have a qualified right of access to court proceedings and records. This right is rooted in the common law. The First Amendment also confers on the public a qualified right of access. The process used by courts to keep some of their proceedings and records confidential is generally referred to as sealing. If a proceeding is sealed, often referred to as closed, it is not open to the public. Usually this means that any transcript made of the proceeding will be regarded as a sealed record.

Traditionally, clerks of court protected sealed filings and records by storing them separately from the public case file in a secure room or vault. As court records have become more electronic in form, electronic methods of security have been developed.

ATTORNEYS ROUTINELY FILE CONFIDENTIAL AND SENSITIVE CLIENT INFORMATION

In 2009, the Federal Judicial Center published an expansive list of all materials filed under Seal in the federal courts. The paper identifies an astonishing number of areas, too extensive to list here, with a Table of Contents that goes on for several pages.

Examples include: Sealed Civil Cases, Qui Tam Actions, Sealed Pending Government's Decision Whether to Intervene, Sealed Pending Settlement, Filed Under the Miller Act, Habeas Corpus Actions and Prisoner Petitions, Cases Concerning Minors and Childhood Sexual Abuse, Cases Involving Confidential Business Information, Medical Information, Confidential Settlement Agreements, and on and on.

Almost all attorneys will have the need to file sealed documents in their practices, some frequently and some occasionally.

MOST SEALED DOCUMENTS RISK BEING UNSEALED FOR A VARIETY OF REASONS

Most sealed pleadings and documents risk being unsealed, i.e., most client confidences that are filed with the court as well as private consumer information, risk being made public unless the attorney takes affirmative steps to protect it.

Wikihow sets for the general rule: "Generally speaking, all court proceedings in the United States are open to the public. This openness extends to court records, which the public has a right to inspect. However, court records can be "sealed" (closed to the public) for a variety of reasons. For example, a court will seal records that relate to juveniles or that reveal a business's trade secrets. It can also seal records that contain sensitive national-security information. If you want to have particular court records unsealed, you will need to submit a request to the court where the sealed records are held."

2 https://www.law360.com/articles/772291/law360-reveals-400-largest-us-firms
3 https://www.selectusa.gov/professional-services-industry-united-states

So, anyone asserting public or media access may file a motion with the court to unseal court records and make them public.

In addition to that, all sealed records in some jurisdictions automatically become unsealed under new court rules unless the interested party files a motion to turn over restricted and sealed documents. See this chilling rule adopted in 2001 by the Northern District for Illinois:

"The United States District Court for the Northern District of Illinois recently adopted a policy that could cause public disclosure of documents filed under seal as recently as three months or as far back as 20 years ago. Other state and federal courts could follow suit. [Under this rule,, the] court clerk [is obligated] to maintain and enforce restrictions on filed documents, including a document's seal, for only 63 days following final disposition of a case, including appeals. **Unless a party moves the court within those 63 days to turn over restricted and sealed documents, "at the end of the 63 day period the clerk shall place the restricted documents in the public file."** Upon a motion for return of the restricted
documents, the court may issue an order to have the document returned, destroyed, or retained as a restricted document for a period not to exceed 20 years and thereafter destroyed."

To protect documents filed or lodged under seal, these are the steps being recommended:

STEP 1: Always study a court's local rules and general orders for provisions relating to sealed or restricted documents. The importance of avoiding damaging disclosures even merits a brief telephone call to the court clerk's office after final disposition to ask how the court preserves or disposes of restricted and sealed documents.

STEP 2: Keep your own complete list of sealed and restricted documents containing your client's confidential information, including such documents filed by other parties in the case.

STEP 3: If confidentiality is your client's paramount concern, periodic inspection of the public court file throughout litigation and even after may be prudent. As Salomon Smith Barney illustrates, restricted documents can "find their way" into the public file; it would be better for you to get to them before the news media, a competitor, or litigation opponent finds them.

STEP 4: Immediately when a notice of appeal is filed, scrutinize the appellate court's rules, general orders, and operating procedures for provisions relating to sealed or restricted documents. Contact the appellate court's clerk about any relevant policies and procedures to ensure that protections established in the trial court are maintained.

STEP 5: To avoid the surprise of future purging and disclosure policies, secure the return of all restricted documents after the close of litigation if the court allows it.

The Northern District of Illinois' policy of opening documents filed under seal and making them available to the public presents a new threat to the privacy of litigants. Litigators should recognize that this is a risk they must be ready to address not only in the Northern District, but in all courts, state and federal, and at every level. The best assurance of the security of your clients' documents comes from informing yourself of court rules and policies, working through them to maintain documents as restricted or sealed at every stage and level of litigation, and to secure the return and restrict access to those documents, whenever possible, when litigation has ended."

WHAT DOES THIS MEAN TO LAW FIRMS AND ATTORNEYS?

As stated by the American Bar Association: "The attorney-client privilege is the backbone of the legal profession. It encourages the client to be open and honest with his or her attorney without fear that others will be able to pry into those conversations. Further, being fully informed by the client enables the attorney to provide the best legal advice..."(2)

So what does it mean to the attorney who fails to protect the information covered by this privilege, or the confidential information provided by clients, or private consumer information shared by clients?

Avoid the Domino Effect of Breached Client Confidential Information

Inadequate cyber security leads to a breach or inadvertent disclosure of sensitive client data. This can result in a domino effect:

Domino 1 — Loss of client data = loss of client trust

Domino 2 — Loss of fees, uncollected bills, cash flow issues

Domino 3 — Reputation damage

Domino 4 — Client injury resulting from inadequate cyber security procedures and protocols

Domino 5 — Legal malpractice and disciplinary action

Wikilocks stops the disastrous domino effect by stopping the first domino from falling.

What starts as an inadvertent disclosure can result in a violation of the attorney's ethical and legal obligations, potential disciplinary action by the bar, potential legal malpractice claims by clients, embarrassment and damage to reputation, loss of existing clients and inability to attract clients in the future, not to mention **risk to collection of fees from existing clients** if they become aware a duty to protect their confidentiality and privacy has been breached. This can also bleed into existing healthy client relationships if word gets out that their information might also be at risk due to inadequate protection issues.

WikiLocks Security is designed to address these potential problems by providing a simple and affordable means by which confidential information can be collected, stored and shared during and after a litigation process, without the need for IT intervention or lengthy implementation projects.

1 https://en.wikipedia.org/wiki/Information_privacy_law
2 https://www.americanbar.org/publications/blt/2013/10/01_unger.html

ABOUT WIKILOCKS:

As cyber-attacks are increasingly sophisticated and a persistent threat to every individual, business, and organization. The typical industry response is to lock the data down with more restrictive governance policies and security controls. However, when information assets are restricted, the effectiveness and efficiency of a business is significantly impacted. With information being the life blood of an organization, it needs to flow to customers, employees, and business partners. This challenging misalignment of security to business process leaves us with either too much or too little security. The industry lacks a solution that addresses the protection of the content, "the data"... Until Now!

WikiLocks is an innovative content security platform that allows for the movement and sharing of information without altering the way you do business. WikiLocks simply applies encryption to specific portions of sensitive content within unstructured data formats such as documents, emails, text, and images. Business and individuals can now allow information owners to properly classify and protect their sensitive content to protect the business. Using a simple "Select— Protect — Distribute" philosophy, WikiLocks leverages the user's knowledge and skills of the most common business applications to protect content such as personal identifiable information, company secrets, or client-attorney privileged information to dynamically enhance the privacy and security of your business.