SLW INSTITUTE
Building Extraordinary IP Assets

Key Topics Webinar Series

Navigating Security Risks When Using Third Party Practice Tools

Before We Get Started...

Recording

A link to the recording and slides will be emailed to all registrants.

Questions

Type in the question box and we will answer in real time or during the Q&A.

Social

Follow us on LinkedIn or go to SLW Institute on slwip.com to see upcoming and on demand webinars.

Today's Presenters…

Steve Lundberg
Principal & Chief Innovation Officer
Schwegman Lundberg & Woessner

Shebli Mikailli
Principal
Schwegman Lundberg & Woessner

Tom Ernster
Director of Information Technologies
Schwegman Lundberg & Woessner

Third-Party Practice Tools

- **Provide assistance and increase efficiency when preparing and prosecuting patent applications**
  - Review Patent Claims/Specification
  - Automated Patent and Figure Drafting
  - Docket Management

- **Present potential security and data privacy risk**
  - Providing confidential data (claims, specifications) to a third-party
  - Confidential data is accessible via the cloud

What is Privacy Law?

- **Privacy law** is the body of law that deals with the regulation, storing, and using of personally identifiable information, personal healthcare information, and financial information of individuals, which can be collected by governments, public or private organizations, or other individuals.
- Also applies to trade secrets and the liability that directors, officers, and employees have when handing sensitive information.

Origins of US Privacy Protection

- **Constitutional Law –** 4th Amendment governs our privacy against unreasonable search and seizure
- **Tort Law** – Invasion of Privacy
- **Contract Law** – Breach of contractual obligation to maintain privacy

Evolution of US Privacy Law

- Privacy law has evolved in response to societal and technological changes
  - Changes in types of data, how data is shared, managed, and used.
- **1890 –** "The Right of Privacy" published in response to invention of photography and scandalous articles being written by journalists
- **1986 –** Computer Fraud and Abuse Act - prohibits accessing a computer without authorization
- **2014 –** Supreme Court ruled that police must obtain a search warrant to search a suspect's phone

Data is changing at a rapid rate

- Format of data – Digital versus physical
- Accessibility and ease of transporting data and collecting data
- Types of data collected has expanded – Browsing history, geographic location, biometric data, social networking data
- The rate at which data is collected and transmitted is increasing
- Data is increasingly being monetized to provide directed marketing, advertising, etc.
- Types of devices that collect data is increasing

Data Privacy is a growing concern

- Several high-profile data breaches and privacy violations have raised national concerns
- Estimated that a majority of Americans have experienced some form of data theft or fraud
- Rising concern related to both government and private sector collection and use of data
- Increasing number and types of attacks

Target Data Breach - 2013

- Cyber Attackers gained access to a customer service database, installed malware on the system and captured full names, phone numbers, email addresses, payment card numbers, credit card verification codes, and other sensitive data of 60 million Target Customers.

Equifax Data Breach - 2017

- Cyber attackers gained access to Equifax's systems and over a 76 day span were able access private records for 147.9 Million Americans, 5.2 million British citizens and about 19,000 Canadian citizens
- Represents about 45% of the US population.

Facebook/Cambridge Analytica – 2010s

- Personal data belonging to millions of Facebook users was collected without their consent by British consulting firm Cambridge Analytica, predominantly to be used for political advertising
- The data was collected through an app called "This Is Your Digital Life", which consisted of a series of questions to build psychological profiles on users and collected the personal data of the users' Facebook friends via Facebook's Open Graph platform.
- The app harvested the data of up to 87 million Facebook profiles

Facebook/Cambridge Analytica – 2010s

- The data was used to provide users with targeted political advertisements. Both Ted Cruz and Donald Trump used these services as part of their campaigns.
- They had a model that could automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender

Facebook/Cambridge Analytica – 2010s

- “The researchers note that "less than 5% of users labeled as gay were connected with explicitly gay groups," but that liking "Juicy Couture" and "Adam Lambert" are likes indicative of gay men, while "WWE" and "Being Confused After Waking Up From Naps" are likes indicative of straight men. Other such connections are peculiarly lateral, with "curly fries" being an indicator of high IQ, "sour candy" being an indicator of not smoking, and "Gene Wilder" being an indicator that the user's parents had not separated by age 21.”

Law Firm Breaches

- Hackers frequently target law firms because of the valuable client data they acquire and retain in the scope of representation (e.g., trade secrets, financial data, and sensitive personal information).
- In December 2016, a team of three hackers was charged with hacking into at least seven law firms to obtain insider information on merger and acquisition deals.
- Over eight days, they collected 40 gigabytes of confidential information, guiding an investment strategy that yielded a profit of $4 million

What Laws Govern Data Protection & Privacy?

- United States – Combination of Federal and State laws
- European Union (EU) – General Data Protection Regulation (GDPR)

What is Generally Covered by Laws

- Scope – What is being regulated, who are Covered businesses, who is protected (consumer)
- Defines the covered personal information
- Disclosure/Notice Requirements
- Consumer Rights (opt out, non-discrimination)
- Mechanism to Access Data (Consumer Requests)
- Enforcement, Remedies, Data Breach

Common Themes and Approaches

- It’s not a matter of if, but when – there’s no such thing as infallible security.
- Requirements aren’t to guarantee perfection, but rather to implement reasonable security - build reasonable protections, take reasonable steps, and be prepared.
- What constitutes Reasonable security is constantly changing and the bar is increasing

Reasonable Industry Standard

- There are standards organizations that provide guidelines and frameworks for data security
- National Institute of Standards and Technology (NIST)
- Cybersecurity Control Frameworks
- International Standards Organization (ISO)

What is a Standard/Framework?

- Details requirements for establishing, implementing and maintaining an information security management system to help organizations secure information.
- Examining risks
- Designing/implementing security controls
- Adopting an overarching management process
- An organization can be certified as compliant if requirements are met.

Practical Guidance on Evaluating Tools

A Solid Framework: ISO 27001/27002

- ISO 27001 provides requirements for an infosec management program whereas ISO 27002 offers guidance focused on implementing specific security controls
- Pay attention to **ISO/IEC 27017**:2015 “Code of practice for information security controls based on ISO/IEC 27002 for cloud services.”
    - Traditional on-premises tools can also be ‘cloud-enabled’ tools based on your licensing or subscription model. E.g., Acrobat, ChemDraw, etc.
    - Defn. A ‘control’ is a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of information. -NIST
    - 27017 covers cloud-specific concepts and includes guidance for select controls in ISO 27001/27002 with additional controls related to cloud services.

ISO 27017 Concepts:

- Both the cloud service and the customer should have a risk assessment and risk handling process.
- Supplier risk should address the use of cloud services and the larger supply chain.
    - “Cloud service customers and cloud service providers can also form a supply chain”
    - e.g., Have you considered the cloud services your suppliers are using, do you know how they manage risk, and how that could impact your organization?
- Firms should manage gaps between their infosec requirements and the capabilities of their cloud services.

ISO 27017 Obligations:

- Apply common security controls to cloud environments
- Ensure information security and risk management processes apply to cloud services
- Have a separate cloud computing information security policy
- Ensure cloud providers' procedures align with your organization's requirements
- Review cloud provider agreements to define roles and responsibilities

ISO 27017 and New Cloud-Related Controls

- Define and document shared information security roles
- The timely removal / return of assets upon termination
- Ensure segregation of virtual environments
- Harden virtual machines in cloud environments
- Define and monitor procedures for administrative operations
- Ensure your ability to monitor aspects of the cloud service
- Ensure consistency of configuration between virtual and physical networks

Risk Management & Supplier Assessment

- Look to ISO/IEC 38500:2015's six overarching principals

1. Responsibility: Define roles and responsibilities within your firm and shared responsibilities with your cloud provider.
2. Strategy: How does the cloud service support the broader objectives of your firm?
3. Acquisition: What do you consider before you buy the service?
4. Performance: Monitoring the cloud service for service deliverables and continual risk assessment.
5. Conformance: Impacts on legal, regulatory contractual and organizational goals.
6. Human Behavior: Talent / Awareness

Practical Advice

- Map your data!
- Create checklists and determine what you need to know before you buy
- Engage your management and compliance teams
- Educate decision makers and build a culture that loops-in your IT and compliance people.
- Set guidelines for evaluating cloud services
- Know your regulatory obligations and your client needs before you commit
- If in doubt write it out – but write it out anyway. Contracts!
- Know your exit strategy!
- Make sure everyone understands their roles and responsibilities, both in your organization and at the provider. This should include your legal, technical, and operational teams.

Guidelines for Those Purchasing Tools

Ask the provider if they offer:

- Recent third-party risk assessments or attestation of their security and privacy posture
- References to security and privacy frameworks, standards or accompanying certifications
- A least-privilege, role-based security, and administrative model
- Data retention, expiration and litigation hold capabilities
- Strong authentication policies and identity service integrations
- Data isolation from other companies (or tenants)
- Encryption at rest and in transit as well as key management
- Data locality options (including data accessibility options)
- An incident or breach response policy defining timing, notice, contacts, and roles
- Advanced notice prior to changes in privacy and security policy or delivered service
- Strong logging, auditing, and reporting!

Additional Guidelines, Considerations & Hidden Costs

- Does the provider have their own cyber insurance?
- Review your contracts and involve your general counsel
- Consider SLAs (Service Level Agreements) and how availability impacts your organization
- Consider impact on your systems or infrastructure
- Consider unexpected data locations
- Does the provider offer a method to classify data?

Sample Assessment Checklist

Cloud Vendor Assessment

NOTE: The word 'app' is referring to the application or service provided.

Does the service comply with the following standards, frameworks, or regulations?

Standard	Description	Compliance %, Y/N or N/A
FINRA	A standard set for not-for-profit organizations author enforc and m	
FISMA	US legi frame operat against	
GAAP	A colle rules a	
HIPAA / HITECH	US legi the co identif Entity : PHI sha	
GLBA	The Gr also kn 1999. I require share a inform Affiliat PII sha	

Does the service or application support the following controls or technologies?

MFA / 2FA Support	Does the application or service support multi-factor authentication? If so, how?	
Same Sign-On Support with Azure AD?	Does the application support single sign-on or same sign-on identity and federation with Azure AD? If so, what protocols and to what extent?	
IP address restriction	Does the app support IP address	
Audit trail		
Admin audit trail		
Data audit tr		

Recommended Contractual Provisions

Security Requirements	Policies/standards, security program, security contact, incident response, data breach disclosure, audit/assessment rights, vulnerability management, secure architecture/development practices, virus/malware scanning, secure network, remote access, identity and access management, physical security, data destruction, business continuity/disaster recovery, independent certifications, background checks
Privacy Requirements	Compliance requirements, other requirements (e.g. PCI), definitions of sensitive or personal information, data breach notification cost allocation, credit monitoring cost allocation, explicit privacy requirements (notice, consent, choice, collection/proportionality, use, transfer, processing, retention, deletion), data breach public notice rights
Other Legal	General confidentiality clause, applicability to affiliates or other legally connected parties, sub-contractors or processor responsibilities, insurance coverage (e.g. cyberliability limits), financial viability requirements, liability limitations/allocation, third party beneficiaries, applicability after service (continuing obligations), severability and modification clauses

A few (or more) words

- MFA/2FA
- Encryption
- Security by Platform
- Government clouds

> “I felt exactly how you would feel if you were getting ready to launch and knew you were sitting on top of 2 million parts — all built by the lowest bidder on a government contract.” - Attributed to John Glenn

Solutions to Secure Cloud-based Tools

- CASB (Cloud Application Security Broker)
  - Microsoft Cloud App Security
- Hybrid, managed SIEM, MDR or MSSP solutions
  - E.g., Palo Alto Prisma Cortex, Crowdstrike, Azure Sentinel, Esentire, Arctic Wolf, etc.
- Identity Providers
  - Azure AD P2, Okta, OneLogin, DUO Security, and more…
- Others…

Resources

- Cloud Security Alliance https://cloudsecurityalliance.org/
- Cloud Control Matrix
- Consensus Assessment Initiative Questionnaire (CAIQ)
- ISO https://www.iso.org/standard/43757.html
- NIST https://csrc.nist.gov/

Patent Drafting Tools

Patent Drafting/Proofreading Tools

- Patent Bots
- Patent Optimizer
- Patent Advisor
- Rowan Patents
- ClaimMaster

Patent Bots

Patent Bots is Safe and Secure

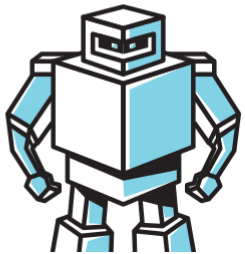
Who We Are

Patent Bots is run by Jeff O'Neill, a practicing patent attorney, who was previously patent counsel for Amazon, an associate at a Boston patent firm, and a clerk for the First Circuit Court of Appeals. Jeff also knows web security having run a secure online voting website for more than 9 years. See Jeff's resume on LinkedIn.

We Don't Store your Patents

You are likely already storing your patent documents in the cloud, such as by emailing drafts to clients or using cloud storage within your firm.

We don't. We process your documents in seconds and immediately discard them. We don't store or log any content of your documents.



Security Practices

We use best practices for security. See below for our grades from several third-party evaluations along with comparisons to other cloud services you may use.

Here are some examples of our security practices:

- We encrypt communications using both HTTPS and HSTP.
- We don't store any sensitive information, such as credit card numbers (we rely on established providers of payment services).
- We use a strong, unique password and two-factor authentication to access our servers.
- All servers are located in the United States.
- We run on Google Cloud Platform and Amazon Web Services to make sure that our servers have the latest security updates.
- We run weekly vulnerability scans to vet our security practices. Contact us if you would like see a copy of a recent report.

Security Test	Patent Bots	Gmail	Drop Box
Mozilla Observatory	A+	A	C-
SSL Labs	A+	A	A+
ImmuniWeb	A+	A	A
Security Headers	A+	A	A

Click any of the grades to see detailed results.

https://www.patentbots.com/security

Patent Optimizer

LexisNexis

Information Security

PatentOptimizer is a client-side software solution which contains some functionality that securely connects over the internet to our server, having a web address of https://www.lexisnexis.com/epact and a static IP address of 138.12.4.174, via a bidirectional encrypted communication protocol using Transport Layer Security (TLS)/Secure Sockets Layer (SSL) on port 443.

A valid digital server certificate issued by Trustwave® (a trusted certificate authority and global leader in next generation server security and compliance) is used to establish the secure connection between PatentOptimizer and our web server.

Data Transmission

There are limited instances in which PatentOptimizer communicates with our secure server via a bidirectional encrypted communication protocol, examples of which are outlined in the chart below.

Patent Application Data Protection

PatentOptimizer is a client-side software solution that analyzes the specifications, drawings, and claims of draft patent applications on the subscriber's local machine. **Accordingly, PatentOptimizer does not transmit the specifications, drawings, and claims of draft patent applications being analyzed to our secure server over the internet. Therefore, in the unlikely event that an encrypted communication were to be compromised, the hacker would not be able to determine the scope of the invention recited in the claims, described in the specification, or illustrated in the drawings, of the corresponding draft patent application being analyzed**.

Our Security team regularly conducts vulnerability and penetration testing. In addition, there are no "backdoors" enabling unauthorized access to PatentOptimizer, which has been in commercial use by thousands of users from Am Law 100 and 200 firms, and Fortune 500 companies, for over 15 years without incident.

See https://www.lexisnexis.com/en-us/terms/privacy-policy.page and the LexisNexis PatentOptimizer - Technical Guide

Patent Optimizer

LexisNexis

Exemplary Instances of Encrypted Communication with our Secure Server
ID Activation/Deactivation
ID/Password Authentication
Software Updates
Retrieving **Image File Wrapper (IFW) Documents and Application Data** from the USPTO Public/Private Patent Application Information Retrieval (PAIR) system for incorporation into the Office Action Response (OAR) tool
Retrieving **File History Information** from the USPTO Public/Private Patent Application Information Retrieval (PAIR) system for incorporation into Term Analysis Reports
Retrieving **Bibliographic Citation Information** of cited references, including domestic and foreign granted patents and pre-grant published patent applications, during generation of USPTO Information Disclosure Statements (IDS) using Check References
Retrieving **Post-Issuance Activity Information**, including **Legal Status** and **Assignment** information, when generating a Check References Report using Check References
Retrieving **Court Docket Information** from CourtLink
Retrieving desired **Image File Wrapper (IFW) documents** via the USPTO PAIR system using Check References and the Office Action Response (OAR) tool
Analyzing public patent documents (public) including domestic and foreign granted patents and pre-grant published patent applications, in Analytics to **Identify Specific Items of Interest** (e.g., people/organization, domestic/foreign patent classification, filing/publication date, terms/phrases, part expressions, claim elements, patent citations, thesaurus variants, patent images, part name/number indices)
Retrieving information from our proprietary **Means Plus Function Thesaurus**
Retrieving **Art Unit Predictive Analytics** information from a complimentary slice of LexisNexis Pathways®

Patent Advisor

LexisNexis

LEADING SECURITY

Keeping your data safe

We understand the utmost importance of protecting confidential information, from private patent application data to searches and saved results. We further protect any private patent information you have entrusted us with using state of the art encryption technology. Your private data is encrypted both in transit and at rest using AES256 bit encryption.

PatentAdvisor™ enhances security by:

- Rigorous system security controls and procedures
- Regular, independent audits

Information Security Management
ISO 27001
www.dekra-seal.com
DEKRA certified

PatentAdvisor™ is the only prosecution solution to maintain an ISO 27001 Certification

www.lexisnexisip.com/products/patent-advisor/

https://rowanpatents.com/drafting/

Rowan Patents

Management's Commitment to Security

Rowan Patents security begins with a demonstrated commitment at the top levels of management to protect your data in the service. Our security team meets weekly to discuss existing controls and procedures and how to improve them.

The Rowan Patents engineering team regularly conducts detailed, security-led assessments of our services and applications for vulnerabilities that could impact the security of customer data. The engineering team continually evaluates new tools to improve our security frameworks and infrastructure.

Data Security in Transit

All communication between Rowan Patents client and servers is conducted through HTTPS. We support Transport Layer Security (TLS) 1.2. We allow only high-strength cipher suites to be negotiated, and we explicitly disable any protocols known to be insecure. All PKI Certificates use 2048-bit keys, in line with industry best practices. We also enable HSTS (HTTP Strict Transport Security) to protect clients from malicious actors who may attempt to downgrade security, and we support Forward Secrecy.

Data Security at Rest

All Customer Data on Rowan Patents is stored encrypted at rest using industry-standard 256-bit AES. However, Rowan Patents has designed its products to avoid or limit storage of sensitive client data. Please see the product-specific details for more information.

Physical Security

Rowan Patents uses Amazon Web Services (AWS) as its sole cloud provider. AWS provides an ISO 2700 (NIST Special Publication 800-132) and SOC 2 compliant data center (AWS Compliance). Rowan Patents stores data only on those AWS services that are covered by AWS's ISO 27001 and SOC 2 certifications.

Rowan Patents

https://rowanpatents.com/drafting/

Data Location

All of Rowan Patents servers operate in the AWS us-east-1 region, which is located in Northern Virginia (though some data in this region may be stored in the Pacific Northwest). All data (including backups) within an AWS region is isolated to that region, and AWS doesn't replicate data automatically across regions (AWS Regions and Availability Zones).

We make it a priority to ensure that customer data is not stored or transferred across national borders.

Account Security

Rowan Patents never stores your password in plain text. We store account passwords using the PBKDF2 algorithm with a unique salt for each credential, as recommended by NIST 800-1321. PBKDF2 makes brute-force attempts and guessing passwords computationally infeasible, while the unique salts used for each credential render common pre-computational attacks such as rainbow tables completely ineffective.

Rowan Patents web applications use session authentication for authorization. Session cookies can be accessed from HTTPS only (not HTTP or Javascript). Mobile and desktop clients use OAuth for authentication. Under no circumstances do our web or desktop applications store your password on your browser or device.

Product Security

At the heart of Rowan Patents security is a robust application architecture that is designed from the ground up to protect your data.

Our security begins with selecting tools that have robust mechanisms to protect against common application security issues including CSRF, XSS, SQL injection, session hijacking, URL redirection, and clickjacking. We have a robust suite of tests to ensure code quality, and our engineers are educated on how to test and spot security errors.

Rowan Patents client uses a well-defined REST API to access data within your account. An integral part of this API is a robust authorization layer that ensures only you can access your data. Authentication credentials (OAuth access token or session token) are checked on every object access.

In certain circumstances, clients access objects directly from Amazon S3. These objects are always accessed by HTTPS, and URLs to objects in S3 are protected by OAuth 1 signatures and are valid for only a short period of time after they were issued.

ClaimMaster

How does ClaimMaster compare to competitor products?

When it comes to core proofreading and automation features, we offer the same or better functionality than our competitors, but at a fraction of the cost. Unlike our competitors, we are a small, independent company that operates without significant overhead and can quickly address any issues or suggestions you may have. ClaimMaster is our only product and we are continuously improving it. We are also not trying to use our product to upsell you other products, such as a subscription to LexisNexis. Nor does our software require you to upload your highly confidential patent documents into the 3rd party cloud for proofreading or drafting, where they will be exposed to numerous serious security risks.

Is there a cloud-based version of ClaimMaster?

No. While the cloud-based systems may seem to offer easier updates and deployment, we do not believe they are the right choice for proofreading patent applications. In the patent world, theft or unintentional disclosure of unfiled patent applications can have very dire consequences for the IP owners, especially in the countries with first-to-file systems, including the United States. In addition, uploading confidential patent documents into the 3rd party cloud for proofreading may raise attorney-client privilege and confidentiality issues. However, because ClaimMaster is an add-in to Microsoft Word, it executes locally on your computer and does not introduce additional security risks, such as the ones created by cloud-based systems. In addition, because ClaimMaster is fully integrated with Word, it works with native Word formatting and offers many unique Word automation features that are not available from the cloud-based systems.

SLW SCHWEGMAN LUNDBERG • WOESSNER

Questions?

These materials are for general informational purposes only. They are not intended to be legal advice, and should not be taken as legal advice. They do not establish an attorney-client relationship.

SLW INSTITUTE
Building Extraordinary IP Assets