Using Artificial Intelligence to Manage Legal Risk by Detecting Anomalies

ABA Cyberspace Law Institute/Winter Working Meeting
January 26-27, 2018

Alexandra Villarreal O’Rourke, Partner, McGuireWoods LLP, Charlotte, NC
Lisa Lifshitz, Partner, Torkin Manes LLP, Toronto, ON, Canada
Richard C. Balough, Principal, Balough Law Offices, LLC, Chicago, IL

The SEC, FTC, and other governmental agencies are implementing the use of artificial intelligence to detect anomalies such as flagging trading patterns and identity theft. As the agencies begin to implement artificial intelligence for regulatory oversite, do companies also need to implement artificial intelligence for red flagging potential issues? If companies adopt artificial intelligence to red flag anomalies, then have they set a higher standard of care to detect such abnormal activities? The presentation will be the starting point for a roundtable discussion.
Using Artificial Intelligence to Manage Legal Risk by Detecting Anomalies

Alexandra Villarreal O’Rourke
ao’rourke@mcguirewoods.com
Key Terms

- Artificial Intelligence
- Machine Learning
- Deep Learning
- Neural Networks
Natural Language Analysis

- Can detect common "topics" among similarly unrelated documents and communications

- Can detect "tonality" to determine whether the language gives signals of anomalies

- "Sentiment analysis" can predict individual and group wrongdoing
Natural Language Analysis

IBM Watson Trader Example

• U.S. traders stopped using angry language and profanity before engaging in wrongdoing (the “act natural” effect?)

• U.K. traders, by contrast were more likely to use profanity when engaging in wrongdoing

• The system learned to identify linked groups by “digital high fives” after wrongdoing
Detecting Deviations from the Baseline

- AI models can learn what is “normal” for a person, a group, a system, etc.
- They can adjust for dynamic baselines
- By learning what is normal, these models can very accurately predict when something is “not quite right”
- New systems give the user a way to prioritize by detecting the level of rarity and the potential importance of an anomaly
Sample Laws Involving Anomaly Detection

- Unfair and Deceptive Acts and Practices laws
- Cybersecurity Breach Laws
- Identity Theft “Red Flags Rules”
- SEC Fraud Detection Requirements
Unfair, Deceptive, or Abusive Acts or Practices (UDAAP)

• Can hold companies responsible for employee wrongdoing

• Creates implicit requirement to monitor for malfeasance

• Example: Ocwen mortgage servicing errors
Cybersecurity

- The Federal Trade Commission has brought a number of enforcement actions on the failure to prevent data breaches.

- It describes companies’ duties in this area as follows: “a company’s data security measures must be reasonable in the light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.”

- EU’s Directive on Security of Network and Information Systems (NIS Directive) requires digital service provider and certain companies “essential for the maintenance of critical societal/economic activities” to ensure state of the art levels of security that will prevent and minimize the impact of cybersecurity incidents on their systems.
Identity Theft

• The FTC & SEC also have “Red Flag Rules” relating to identity theft, which require companies to have “reasonable policies and procedures to identify the red flags of identity theft that may occur in your day-to-day operations. . . . For example, if a customer has to provide some form of identification to open an account with your company, an ID that doesn’t look genuine is a ‘red flag’ for your business.”

• As AI systems become more commonplace, it is likely that this standard will shift towards an expectation of AI use, particularly as AI-based cybersecurity threats grow
SEC’s Requirements

• Securities laws have a number of requirements that place upon covered firms the duty to prevent and detect fraud.

• For example, the SEC Act requires audits that include “procedures designed to provide reasonable assurance of detecting illegal acts that would have a direct and material effect on the determination of financial statement amounts.”

• The SEC also requires “Management’s evaluation of the risk of... the vulnerability of the entity to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets and corruption), and whether any such exposure could result in a material misstatement of the financial statements.”

• “The extent of activities required for the evaluation of fraud risks is commensurate with the size and complexity of the company’s operations and financial reporting environment.”
SEC’s Use of AI

- The SEC recently announced that it is using artificial intelligence to detect red flags that may indicate fraud: “Machine learning algorithms may help our examiners by pointing them in the right direction in their identification of possible fraud or misconduct.”

- Sample use case: Investment advisor reporting
  - They review reporting data using topic modeling and tonality analysis to predict the presence of idiosyncratic risk
  - They have found that this method is 5 times more accurate than random at predicting risk
  - However they warn that they use staff to carefully analyze red flags for false positives

- Presumably the fact that the SEC is now using this technology indicates that they might soon expect companies to have the same level of sophistication in detecting trends
Financial Conduct Authority

The FCA’s Head of Data announced that the agency plans to use "supervised machine-learning" and "unsupervised AI" to detect financial irregularities.

- Specifically mentioned speech-to-text analytics and social media analytics

- Also stated the FCA is looking “Effectively converting, probably initially our regulatory reporting rules, into truly unambiguous rules that machines can interpret and implement directly.”
Best Practices for Implementing AI Solutions

• Adopt a phase-in approach to test the fit

• Incentivize your AI team and service providers to work closely with the lawyers

• Have a plan for periodically testing the model and assumptions

• Have a human “gut check” step wherever feasible to identify false red flags
Legal Uncertainty Remains

• As AI technology evolves, to what extent will "reasonableness" prevention standards mandate its use?
• Will companies have to use AI to see what regulators see?
• Does real-time problem identification require real-time resolution?
• Are you volunteering for a higher standard of care?
  – Example: Technology that allows for accurate anomaly detection might create higher expectations for fraud prevention
Questions or Comments?

www.mcguirewoods.com
Lisa is a partner in our Business Law Group, specializing in the areas of information technology and business law and is the leader of the firm’s Technology, Privacy & Data Management Group.

Lisa has particular expertise in preparing and negotiating technology agreements, including Internet-related, m-commerce and e-commerce agreements, cloud computing agreements (SaaS, PaaS, IaaS), cloud retail agreements, cloud storage agreements, app development agreements, hosting agreements, mobile payment agreements, reseller, distribution, outsourcing, system acquisition, maintenance and support agreements, master services agreements and consulting and services agreements. She provides technology-related advice on financings and acquisitions, including export control and open source advice on cross-border deals. She also provides guidance on IoT legal matters. Lisa has considerable experience helping non-Canadian companies, especially American entities, create appropriate legal agreements for their entry into the Canadian marketplace.

Lisa also practices in the area of privacy and information management, advising both Canadian and international clients on compliance with Canadian privacy and cybersecurity requirements. She routinely advises clients on trans-border data transfers, data breach management, privacy compliance in corporate transactions and negotiations, and privacy due diligence in connection with information technology transactions. She frequently provides privacy advice in the healthcare and long-term care sector. She also advises on compliance relating to Canada’s anti-spam legislation.

Publications & Presentations
Lisa currently writes the “IT Girl” technology column for Canadian Lawyer and has authored numerous articles for such publications as Business Law Today, Internet and E-Commerce Law in Canada, e-Commerce Law Report and the BNA International World Data Protection Report. Lisa is also a frequent speaker on technology law issues for organizations such as the American Bar Association, Lexpert, the Canadian Technology Law Association (formerly the Canadian IT Law Association), the Ontario Bar Association, the Law Society of Upper Canada, and the International Technology Law Association.
Memberships

- American Bar Association, Business Law Section, Council Member
- American Bar Association, Science and Technology Section, Council Member
- American Bar Association, Member, ABA Cybersecurity Legal Task Force; co-author Vendor Contracting Project: Cybersecurity Checklist (2017)
- American Bar Association, Business Law Section, Cyberspace Law Committee, Co-Chair of the Robotics and Artificial Intelligence Subcommittee
- American Bar Association, Business Law Liaison to the ABA Standing Committee on Technology and Information Systems (SCOTIS)
- American Bar Association - Science and Technology Section, Editorial Board, The Sci-Tech Lawyer
- Canadian Technology Law Association, Past President and Director, October 2013 - October 2017
- American Bar Association, Member, American Bar Association - Business Law Section, Past Chair, Technology Committee, August 2014 - August 2017
- American Bar Association - Business Law Section, Cloud & IT Services Subcommittee, Cybersecurity Subcommittee, August 2016 - August 2017
- American Bar Association - Business Law Section, Past Member, Editorial Board, Business Law Today, August 2014 - August 2017
- American Bar Association, Past Liaison to the Science and Technology Section and the Business Law Section, August 2011 - August 2014
- American Bar Association, Past Vice-Chair, Cyberspace Law Committee, August 2008 - August 2011
- Toronto Computer Lawyers Group, Past Treasurer, Chair and Vice-Chair, Toronto Computer Lawyers’ Group, 1999 - 2002
- Ontario Bar Association, Past Chair of the Executive of the Information Technology and Electronic Commerce Section, 2006 - 2007
- iTechLaw (formerly the Computer Law Association), Past Director, 2001 - 2007
- iTechLaw (formerly the Computer Law Association), Co-Chair of the Publications Committee, 2002 - 2006
- iTechLaw (formerly the Computer Law Association), Member, Planning Advisory Committee, iTechLaw 2003 World Computer and Internet Law Congress 2002 - 2003

Community Involvement

- Director, Jane Goodall Institute of Canada, 2015 - 2017
- Director, SIM-one, Ontario Simulation Network, 2013 - 2014
- Honourary Past Chair, Corporate Cabinet, The Shoppers Drug Mart Weekend to End Women’s Cancer & Torkin Manes LLP Team Captain, 2011 - 2015
- Director, Bruce Trail Association, Toronto Section, 2011 - 2014
- eHealth Ontario, Director, 2009 - 2010
- Past President of the Board of Directors, Children's Aid Society of Toronto (CAST), 2007 - 2009
- Director-at-large and member of the Executive Committee, Ontario Society for the Prevention of Cruelty to Animals (O.S.P.C.A.), 1997 - 2004

Recognition (con'td)

- The Canadian Legal Expert Directory - “Repeatedly Recommended/Leading Lawyer” in the fields of Computer & IT law and Technology Transactions (2014 - present)
- Ranked by Chambers Global as a "Notable Practitioner" (Band 3) for Information Technology Law in Canada (2010)
Alexandra’s practice focuses on financial services litigation as well as state and federal financial regulatory matters and investigations, including actions taken by the Consumer Financial Protection Bureau (CFPB). She also has significant expertise on Fintech regulatory matters, and co-leads the firm’s Fintech industry group.

Prior to joining McGuireWoods, Alexandra was Senior Counsel with the CFPB’s Office of Law & Policy in Washington D.C., where she advised the bureau on numerous enforcement and supervision matters. She served as the legal division’s team lead in several rulemaking proceedings and in fair lending civil-rights matters. Alexandra also advised the Bureau on Fintech and alternative credit data issues, issues pertaining to consumers with limited English proficiency, and diversity and inclusion matters. Through her work at the CFPB, Alexandra engaged extensively with other financial regulators and government agencies.

Alexandra also served as an attorney with the Office of the Legal Adviser with the U.S. Department of State, where she advised State on both trial and appellate litigation matters concerning national security and immigration. During that time Alexandra received a superior achievement award and two meritorious achievement awards.

Alexandra is a permanent member of the Fourth Circuit Judicial Conference. She served as a judicial clerk for the Honorable Allyson Duncan of the U.S. Court of Appeals for the Fourth Circuit and Honorable Legrome Davis of the U.S. District Court for the Eastern District of Pennsylvania. As a law student at Harvard Law School, she was a Truman Scholar, Soros Scholar, Harvard Post-Graduate Research Fellow, a Sheldon Travel Fellow, and a recipient of the Hispanic Scholarship Fund Hall of Fame – Brillante Award. Alexandra also served as executive editor for the Harvard Latino Law Review and co-founder of the Harvard Law School Immigration Project.

**EDUCATION**

- Queen’s University Belfast, LLM, International Human Rights and Criminal Justice, 2004
- The University of Texas at Austin, BBA, Finance Honors, B.A. in Plan II, summa cum laude; Phi Beta Kappa, 2003

**ADMISSIONS**

- North Carolina
- U.S. Court of Appeals for the 4th Circuit

**PUBLICATIONS**

- Co-author, "Consumer Financial Protection Bureau Considers the Risks and Promise of Alternative Data in the Credit Context," *ABA Business Law Section, Consumer Financial Services Committee Newsletter*, June 2017
EVENTS
• Moderator, Black Box Boom - How Artificial Intelligence is Reshaping Financial Services, Charlotte, NC, August 29, 2017
• Panelist, "New Data, New Payments," Let’s Talk Payments, August 8, 2017

AFFILIATIONS
• Fellow, American Bar Foundation, 2017-2019

LANGUAGES
• Spanish

The McGuireWoods website provides information of general interest to the public. The website does not offer legal advice about specific situations or problems. You should consult a McGuireWoods lawyer if you have legal issues requiring attention. Nothing on this site creates an express or implied contract. McGuireWoods does not intend to create an attorney-client relationship by inviting you to contact us. Unless and until we and you agree that we will represent you, we will not have any duties to you, including any duty to keep what you send us confidential or any duty to protect your interests. This means that nothing you send us will be kept confidential, unless we mutually agree that we will keep it confidential. Past legal successes described on this website are not indicators of future results. The outcome of particular legal matters is dependent upon the facts and law applicable to the matters.