SQUIRE PATTON BOGGS

Artificial Intelligence Law for In-House Counsel

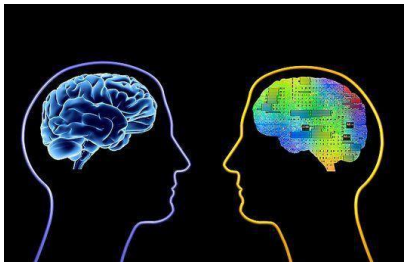
Katharine J. Liao
Stephanie Niehaus
Huu Nguyen

Scope of Talk

SQUIRE PATTON BOGGS

Scope

- Intro to AI
- AI law basics
- AI in the Workplace
- Contractual considerations
- Regulatory concerns
- Ethics and Bias



We won't talk about

- Cyber law, data privacy, OSHA and other robot and drone standards, or AI speech issues

What is artificial intelligence and what are related legal challenges?

SQUIRE PATTON BOGGS

What is AI?

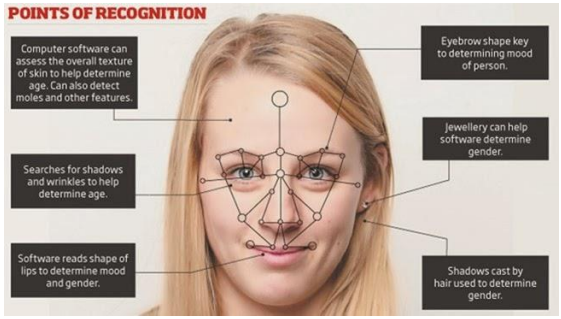
- Application of software that mimics human intelligence to perform tasks normally performed by people

Legal Challenges and Framework

- How to apply existing laws to new problems posed by AI?
- How is AI usage regulated?
- How to contractually limit AI risks?

AI in the legal industry

- E-Discovery
- AI diligence
- Chatbot Lawyers
- HR hiring assistants
- Datamining
- Bio-metric security



AI Law Basics
Tort Liability – Where is the Fault Line?

SQUIRE PATTON BOGGS

- Under a traditional framework, when someone is injured using a product, product liability law determines when and to whom liability attaches
- Product liability is a creature of state common and statutory law:
  - Negligence (duty, breach, causation, damages)
  - Breach of warranty (merchantability or fitness for a particular purpose)
  - Strict Liability (RST 2d Torts § 402A)
    - Design defect
    - Manufacturing defect
    - Failure to warn

AI Law Basics
Semi-Autonomous vs. Autonomous

SQUIRE PATTON BOGGS

Distinguish:

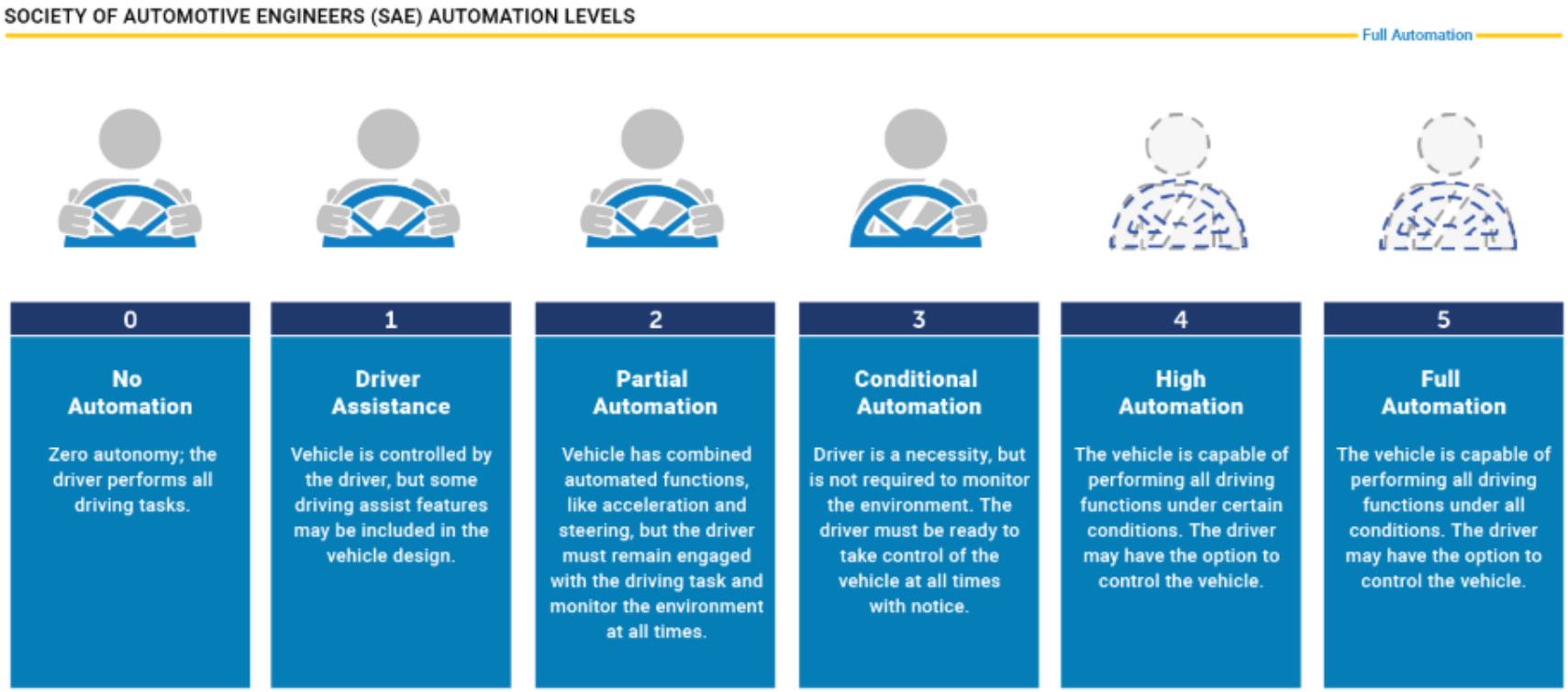
- Semi-autonomous – "the machine functions and makes decisions in ways that can be traced directly back to the design, programming, and knowledge humans embedded in the machine"
- Fully autonomous – the machine functions independently, effectively making its own "decisions" without the direction or intervention of a human being

Vladeck, D., Machines Without Principles: Liability Rules and Artificial Intelligence, Wash. L. Rev. 89:117-50 (2014).

Eran Kahana's classification of Levels A-D apps – from less autonomous to more autonomous. https://web.stanford.edu/dept/law/ipsc/PDF/Kahana,%20Eran%20-%20Abstract.pdf

AI Law Basics
Semi-Autonomous vs. Autonomous

SQUIRE PATTON BOGGS



www.nhtsa.gov/technology-innovation/automated-vehicles-safety

Tort Liability – Where is the Fault Line?

SQUIRE PATTON BOGGS

BUT . . . what happens when we introduce a fully-autonomous machine into the analysis?

- Are fully autonomous “thinking” machines more akin to people, and what does this do to our liability framework?
- Can a machine in and of itself be held “liable,” and who then carries the cost?
- If a machine learns and evolves on its own, is it “substantially unchanged” for purposes of the traditional strict liability analysis?
- How does a machine that learns and evolves on its own impact our notions of foreseeability?

AI Law Basics
Tort Liability – Where is the Fault Line?

SQUIRE PATTON BOGGS

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

Oscar Willhelm Nilsson,
Plaintiff,
vs.
General Motors LLC,
Defendant.

Case No.:
COMPLAINT FOR DAMAGES
1. NEGLIGENCE

JURY TRIAL DEMANDED

15. Defendant owed Plaintiff a duty of care in having its Self-Driving Vehicle operate in a manner in which it obeys the traffic laws and regulations.

16. Defendant breached that duty in that its Self-Driving Vehicle drove in such a negligent manner that it veered into an adjacent lane of traffic without regard for a passing motorist, striking Mr. Nilsson and knocking him to the ground.

17. As a result of such negligent driving, Mr. Nilsson sustained serious injuries of body and mind and incurred expenses for medical care and attendance, all to the great detriment of Mr. Nilsson for past, present, and future damages.

AI Law Basics
Tort Liability – Where is the Fault Line?

SQUIRE PATTON BOGGS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OSCAR WILLHELM NILSSON,
Plaintiff,
v.
GENERAL MOTORS LLC,
Defendant.

Case No. 4:18-cv-00471-JSW

ANSWER AND DEMAND FOR JURY TRIAL

15. The allegations set forth in paragraph 15 of the Complaint are legal conclusions and do not require a response. To the extent a response is required, GM admits that the Bolt was required to use reasonable care in driving, just as Mr. Nilsson was required to use reasonable care in driving his motorcycle.

16. GM denies as untrue the allegations set forth in paragraph 16 of the Complaint.

17. GM denies the allegations set forth in paragraph 17 of the Complaint, insofar as they relate to the nature and extent of Plaintiff's injuries and damages, for lack of knowledge or information sufficient to form a belief about the truth of those allegations. GM denies as untrue the remaining allegations set forth in paragraph 17 of the Complaint.

GM denies all allegations set forth in the Complaint not specifically admitted above.

AI Bias in the Workplace - Fair Credit Reporting Act

SQUIRE PATTON BOGGS

- FCRA also applies to background screening companies and may apply to data brokers.
- FCRA requirements:
  - Consumer Reporting Agencies implement reasonable procedures to ensure maximum accuracy of reports
  - Consumer access to review and correct information
  - Notice if an adverse decision is made based on a consumer report
- Retention of AI data for advice
- How does a consumer review an AI's "file" or get to "dispute incomplete or inaccurate information"?

AI Bias in the Workplace

SQUIRE PATTON BOGGS

- **Now Is The Time To Act To End Bias In AI**, https://www.fastcompany.com/40536485/now-is-the-time-to-act-to-stop-bias-in-ai

- **Example of AI Bias In Recruiting**:
  - Danny Guillory, the head of global diversity and inclusion at Autodesk, came upon the issue while working in the recruiting industry. He offers this example: If you run a search on a professional social network for software engineers, you are most likely to see a first page of results consisting exclusively of Caucasian men. As you engage with the profiles of these candidates, and request more, the AI will deliver candidates with similar attributes to the first wave, very likely resulting in more white men.

Employment Discrimination by Robot?

SQUIRE PATTON BOGGS

- Use of AI algorithm and big data to make employment decisions must still comply with anti-discrimination laws.
- While questions asked by a robot can be pre-screened to ensure legal compliance, disparate impact on protected categories is a big concern. Some features of algorithms may have a disproportionately adverse impact on a protected class. Examples of unintended correlation:
  - Use of certain software may be more common and understandable for younger workers.
  - Data that shows those who have been unemployed as a group are less desirable.
  - Data such as the distance an applicant lives from the potential job site could reflect the different ethnic or racial profiles of the surrounding towns and neighborhoods
  - Data using the reputation of the colleges/universities from which an applicant obtained a degree could have a disparate impact on a protected class if equally qualified members of the protected class graduate from these colleges/universities at a substantially lower rate than those not in the protected class

Calibrating AI to Document Retention Requirements

SQUIRE PATTON BOGGS

- Numerous contrasting document retention lengths for applicant tracking
  - **1 year** – EEOC
  - **2 years** – California, Montana, New Jersey
  - **3 years** – Los Angeles Municipal Code
- Single and Alternate Triggers
  - Date of Receipt or of making the record (Los Angeles)
  - Date of non-hiring (New Jersey)
  - Later of the two dates (EEOC, OFCCP, California, etc.)
- Every time the AI searches the applicant database and decides not to hire, the date of non-hiring resets.

AI and Other Employment Issues – What Is On The Horizon?

SQUIRE PATTON BOGGS

Wage & Hour Issues

- What happens when robots are operated by humans remotely?
- Independent Contractor vs. Employee
- Federal vs. State Wage and Hour Laws
- E-Discovery & Predictive Coding

Health & Safety Issues

- Under the Occupational Safety and Health Act (OSHA), a covered employer utilizing robotics — like any other employer the OSH Act covers — must conduct a "hazard assessment," in which it reviews working environments for potential occupational hazards. 29 C.F.R. § 1910.132(d).
- There are currently no OSHA standards specifically for the robotics industry. However, the OSHA highlights general standards and directives applicable to employers utilizing robotics. See "Robotics, Standards, Occupational Safety and Health Administration, Safety and Health Topics."; see also "Guidelines for Robotics Safety" OSHA Instruction STD 01-12-002 (1987).

AI and Workplace Privacy – Workplace Monitoring

SQUIRE PATTON BOGGS

- **Why Monitor?**
  - Recording activities for training an AI
  - Unknown monitoring by vendors for their own AIs
  - Cybersecurity
  - Protecting company assets and information
- **Mobile devices, IoT devices and tracking.**
  - When can employers monitor GPS and geo track employees?
  - Some states require consent of owner of device or vehicle to track
  - Some states permit employees to sue under common law invasion of privacy or other state privacy laws
  - Medical privacy issues for tracking fitness wearables (e.g., in relation to employee wellness programs)
- **Recommendation:**
  - Use written, disseminated policies to notify employees they will be monitored
  - Narrow employees' expectation of privacy in the workplace
  - Include an acknowledgement by employees that they will be monitored

AI in the Legal Workplace – Best Practices

SQUIRE PATTON BOGGS

- Address diversity and potential discriminatory impact with your HR team, staff and associates and partners
- Don’t depend on technical solutions without understanding how they work
- Be transparent when it comes to privacy concerns and ensure compliance with state laws
- Develop consistent protocol for AI screening while guarding against overbroad AI use
- Hold your AI vendors who provide your HR tools accountable
  - Do you have proper training and support from the AI vendors?
  - Do you and the AI vendors understand the data used to train the AI?
  - Do you have plan of action in case robot misbehaves?

Key Contracting Considerations
Due Diligence for AI Agreements

SQUIRE PATTON BOGGS

- The parties should perform due diligence to confirm, among other things:
  - Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate;
  - Financial status, including reviews of audited financial statements;
  - Service delivery capability, status, and effectiveness;
  - Technology and systems architecture;

Issue

- Does the AI vendor have a compliance program?
- Does the AI provide a mechanism to provide notice to consumers or receive consumer requests for notice and explanations?
- Are the AI's decisions auditable and explainable?
- Does the AI respect regulatory rules?

Key Contracting Considerations Protecting AI Data

SQUIRE PATTON BOGGS

- At least in the Sixth Circuit, confidentiality information can be protected even if not a trade secret. *Orthofix, Inc. v. Hunter*, 2015 U.S. App. LEXIS 20111 (6th Cir. 2015).
- As we have already determined (supra, 8-9), Texas law is clear: "confidential information" is generally defined by the parties, and not by achieving trade-secret status, so long as it does not encompass publicly available information or an employee's general knowledge or skills. … Here, the "confidential information" covered by Hunter's non-disclosure provision does not merely concern publicly available information or Hunter's general knowledge.
- *See, e.g., Corp. Relocation*, 2006 WL 4101944, at *15 n.17 ("Regardless of whether the information contained in the 24 missing files qualifies for trade secret status, the court is satisfied that such information is confidential pursuant to Section 5(a) of the Employment Agreement, to which the parties expressly agreed.")

Issue

- **Protect AI Data both as trade secrets and as confidential information**

Key Contracting Considerations Protecting AI Data

SQUIRE PATTON BOGGS

- Vendor shall protect the confidentiality of Company's Confidential Information during the term of the Agreement and for [___] years thereafter, provided Vendor shall protect the confidentiality of any trade secrets for so long as such Confidential Information remains a trade secret. Except as required by applicable federal, state, or local law or regulation ("Law"), and **except for Company's AI Data which will remain confidential**, the term "Confidential Information" as used in this Agreement shall not include information that falls within the following exceptions ("Confidentiality Exceptions"): … "Comapny's AI Data" means software, unpatented inventions, ideas, methods, and discoveries, trade secrets, know-how, unpublished patent applications, data, corpus, training sets, algorithms, parameters…

Issue

  - AI knowledge is likely based on data observations, which by definition was "known by the public"
  - Take care to anonymized PII in training sets

Key Contracting Considerations Protecting AI Data

SQUIRE PATTON BOGGS

- Defend Trade Secrets Act Notice. Recipient and its personnel are hereby notified that under the Defend Trade Secrets Act of 2016, (a) an individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that: (i) is made (A) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (B) solely for the purpose of reporting or investigating a suspected violation of Law; or (ii) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal; and (b) an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of Law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual (i) files any document containing the trade secret under seal; and (ii) does not disclose the trade secret, except pursuant to court order.

Key Contracting Considerations
Liability Shifting and Indemnification

SQUIRE PATTON BOGGS

- Because it is unclear if a fully autonomous AI agent can be considered negligent or who would be liable for the AI agent's acts, include an express risk shifting in AI agreements
- Consider express allocation of risk via indemnification by the parties
- A party can be indemnified for their own negligence in most states. But intent must be sufficiently clear and unambiguous. *See Stanton v. Oceanside Union Free Sch. Dist*., 32 N.Y.S.3d 620 (2016); *Bradley v. Earl B. Feiden*, 8 N.Y.3d 265 (2007); Levine v. Shell Oil Co., 28 N.Y.2d 205, 212-213 (N.Y. 1971); *Rossmoor Sanitation, Inc. v. Pylon, Inc*., 13 Cal. 3d 622, 628 (1975).

Key Contracting Considerations
Liability Shifting and Indemnification

SQUIRE PATTON BOGGS

- Vendor shall defend, indemnify, and hold harmless the Company, its affiliates, and their respective shareholders, officers, directors, employees, agents, successors, and permitted assigns from and against all Claims arising out of or resulting from (a) any [material] breach of this Agreement by the Vendor; (b) Vendor 's [gross] negligence and willful misconduct; (c) all [proper use] [misuse] of the Products and Services, (d) misuse of Company's data and materials and (e) all data and training provided by Vendor, in each case whether or not caused by the negligence of Company or any other indemnified party.

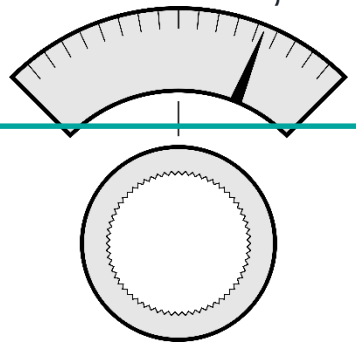
Issue

- **Have broad but enforceable indemnification provisions.**

Key Contracting Considerations
AI Controls

SQUIRE PATTON BOGGS

- Service provider internal controls;
- Compliance with applicable law and regulatory requirements;
- Record maintenance requirements for the service provider, access to records and audit by institution;
- Notification requirements and approval rights for any material changes to services, systems, controls, key project personnel, and service locations;
- Setting and monitoring parameters for financial functions



Issue

- Governmental or consumer complaints about the AI
- Number of “wrong” AI decisions?
- Privacy, security or confidentiality breaches?
- Does the AI satisfy the Company’s own internal policies?

AI Regulatory Concerns
Current AI regulations

SQUIRE PATTON BOGGS

- Very FEW specific AI laws
- SEC guidance on robo-advisors
- Regulators have expressed concerns about AI
- Use analogy to existing human activities under current regulations

AI Regulatory Concerns
FTC and AI

SQUIRE PATTON BOGGS

- The FTC recently had a hearing on AI, and sought public comment on 25 related AI topics at the FTC Hearing #7: Competition and Consumer Protection in the 21st Century https://www.ftc.gov/news-events/events-calendar/ftc-hearing-7-competition-consumer-protection-21st-century
  - What are the main consumer protection issues raised by algorithms, artificial intelligence, and predictive analytics?
  - What roles should explainability, risk management, and human control play in the implementation of these technologies?
  - What choices and notice should consumers have regarding the use of these technologies?

AI Regulatory Concerns
SEC: Robo-Advisors

SQUIRE PATTON BOGGS

- "Automated advisers, which are often colloquially referred to as 'robo-advisers,' represent a fast-growing trend within the investment advisory industry, and have the potential to give retail investors more affordable access to investment advisory services as well as change the competitive landscape in the market for investment advice." SEC Guidance, https://www.sec.gov/investment/im-guidance-2017-02.pdf
- SEC guidance focuses on three distinct areas identified by the Staff, listed below, and provides suggestions on how robo-advisers may address them:
  - The substance and presentation of disclosures to clients about the robo-adviser and the investment advisory services it offers;
  - The obligation to obtain information from clients to support the robo-adviser's duty to provide suitable advice; and
  - The adoption and implementation of effective compliance programs reasonably designed to address particular concerns relevant to providing automated advice

AI Regulatory Concerns
SEC: Robo-Advisors

SQUIRE PATTON BOGGS

- Guidance requires: “The questionnaire eliciting sufficient information to allow the robo-adviser to conclude that its initial recommendations and ongoing investment advice are suitable and appropriate for that client based on his or her financial situation and investment objectives”
- SEC has continually issued guidance for robo-advisors to ensure they are meeting their fiduciary obligations under the Act and other applicable regulations.
- This guidance emphasizes transparency by requiring robo-advisors to disclose their business models and how they utilize consumer data.
- But since robo-advising platforms are based on algorithms, can robo-advisors be induced to make illicit deals or transactions?
- **SEC considers robo-advisers (like human advisor) to have duties!**
- If robo-advisors themselves have duties, do they have independent agency?
- https://news.law.fordham.edu/jcfl/2017/12/29/fi-robot-the-rise-of-automated-robo-investment-advisors/

AI Regulatory Concerns
FCRA, AI notice and records retention

SQUIRE PATTON BOGGS

- From the FTC's summary of consumer rights under the FCRA. https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf
  - Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information

Issues

- Retention of AI data for reporting
- How does a consumer review an AI's "file" or get to "dispute incomplete or inaccurate information"?
- How do you notify consumers when an AI makes an adverse decision?

AI Regulatory Concerns
ECOA, AI Bias and Explainable AI

SQUIRE PATTON BOGGS

- **Big Data A Tool for Inclusion or Exclusion?**
  https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

- Disparate treatment occurs when a creditor treats an applicant differently based on a protected characteristic. For example, a lender cannot refuse to lend to single persons or offer less favorable terms to them than married persons even if big data analytics show that single persons are less likely to repay loans than married persons. Disparate impact occurs when a company employs facially neutral policies or practices that have a disproportionate adverse effect or impact on a protected class, unless those practices or policies further a legitimate business need that cannot reasonably be achieved by means that are less disparate in their impact. For example, **if a company makes credit decisions based on consumers' zip codes, such decisions may have a disparate impact on particular ethnic groups because certain ethnic groups are concentrated in particular zip codes**. **Accordingly, the practice may be a violation of ECOA.** The analysis turns on whether the decisions have a disparate impact on a protected class and are not justified by a legitimate business necessity.

AI Regulatory Concerns
ECOA, AI Bias and Explainable AI

SQUIRE PATTON BOGGS

- **Equifax debuts machine learning-based credit scoring system**. https://www.ciodive.com/news/equifax-debuts-machine-learning-based-credit-scoring-system/520095/:
  - "While other companies use machine learning methodologies in portions of the model building process, the final score is not based on a machine-learning regulatory compliant model … These techniques inherently lack the explain-ability and transparency that is required for compliance and regulatory purposes."
- ***See also* FICO's explainable AI breaks out of the blackbox**. https://www.fico.com/blogs/analytics-optimization/explainable-ai-breaks-out-of-the-black-box/

Issues

- AI decisions creating disparate impact based on impermissible factors
- AI decisions that are explainable to people

New York Algorithmic Decision-making Litigation and Laws

SQUIRE PATTON BOGGS

- New York City's recently passed - A Local Law in relation to automated decision systems used by agencies
  - This bill would require the creation of a task force that provides recommendations on how information on agency automated decision systems may be shared with the public and how agencies may address instances where people are harmed by agency automated decision systems.
  - The term "automated decision system" means computerized implementations of algorithms, including those derived from machine learning or other data processing or artificial intelligence techniques, which are used to make or assist in making decisions.
  - The term "agency automated decision system" means an automated decision system used by an agency to make or assist in making decisions concerning rules, policies or actions implemented that impact the public.
- http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0

CA Bot Disclosure Law

SQUIRE PATTON BOGGS

- Recently passed and will become effective July 1, 2019.
- https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001
  - It shall be unlawful for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election. A person using a bot shall not be liable under this section if the person discloses that it is a bot.
- Arguably could apply to all online bots
  - (a) “Bot” means an automated online account where all or substantially all of the actions or posts of that account are not the result of a person.

Ethics - Black Box AI and Bias

SQUIRE PATTON BOGGS

Black Box AI

- AIs that are trained on massive amounts of data
- Programmers cannot easily extract meaning from the AIs' data

Examples of AI

- Neural network
  - [0.1, 0.2, 0.3] => Offer Promotion
- Probabilistic
  - (0.6, Is Caucasian) => Offer Promotion
- Symbolic/Logic
  - If Person Is Caucasian and Office Is New York => Offer Promotion

Black Box AI and Bias

SQUIRE PATTON BOGGS

Forget Killer Robots—Bias Is the Real AI Danger

- https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/
- Giannandrea who leads AI at Google:

> It's important that we be transparent about the training data that we are using, and are looking for hidden biases in it, otherwise we are building biased systems … If someone is trying to sell you a black box system for medical decision support, and you don't know how it works or what data was used to train it, then I wouldn't trust it.

- Black box machine-learning models called COMPAS predict defendants' likelihood of reoffending, and is used by some judges to determine whether an inmate is granted parole. The workings of COMPAS are kept secret, but an investigation by ProPublica found evidence that the model may be biased against minorities.

Permitting AI Bias In Practice of Law May Be Professional Misconduct

SQUIRE PATTON BOGGS

- ABA Amended Model Rule 8.4(g)
  - Some version of rule adopted in about half of states including New York and California
  - As amended, Model Rule 8.4(g) makes it professional misconduct to:
  - Engage in conduct that the lawyer knows or reasonably should know is harassment or discrimination on the basis of race, sex, religion, national origin, ethnicity, disability, age, sexual orientation, gender identity, marital status or socioeconomic status in conduct related to the practice of law.
- How does this change things? Aren't there statutes addressing discriminatory and harassing practices?
- Do lawyers have a duty to understand and supervise the AI vendors and AI tools that could reasonably be used to cause discrimination?

Norms, Ethics and the Workplace

SQUIRE PATTON BOGGS

- **Tell This Bot About Your Experience of Harassment. It Might Actually Help.,** https://slate.com/human-interest/2018/04/tech-tries-its-hand-at-the-metoo-movement.html
- Motivation: 75 percent of sexual harassment incidents go unreported, according to the EEOC.
- A chat bot Spot uses a cognitive interviewing style - instead of making assumptions about an interviewee's credibility or their story like a non-scripted human might do.
- It's a way of gathering evidence that's more standardized than an untrained HR representative asking questions—which may re-traumatize the victim or impact their retelling of their [harassment] story.
- Once Spot gathers the story, users can decide whether they want to keep it for themselves, or forward a PDF of the story to an HR representative or someone else.

AI and the Duty of Competence Under ABA Rule 1.1

SQUIRE PATTON BOGGS

- Under Rule 1.1 of the ABA Model Rules, a lawyer must provide competent representation to his or her client.
- The rule states that “[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”
- The duty of competence requires lawyers to be informed, and up to date, on current technology. In 2012, this was made clear when the ABA adopted Comment 8 to Rule 1.1 which states that “[t]o maintain the requisite knowledge and skill, lawyers should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . .”

AI and the Duty of Communicate Under ABA Rule 1.4

SQUIRE PATTON BOGGS

- ABA Model Rule 1.4 governs a lawyer's duty to communicate with clients and requires a lawyer to "reasonably consult with the client about the means by which the client's objectives are to be accomplished."
- A lawyer's duty of communication under Rule 1.4 includes discussing with his or her client the decision to use AI in providing legal services.
- A lawyer should obtain approval from the client before using AI, and this consent must be informed.
- The discussion should include the risks and limitations of the AI tool.

AI and the Duty of Confidentiality Under ABA Rule 1.6

SQUIRE PATTON BOGGS

- Under ABA Model Rule 1.6, lawyers owe their clients a generally duty of confidentiality.
- This duty specifically requires a lawyer to “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”
- The use of some AI tools may require client confidences to be “shared” with third-party vendors.
- As a result, lawyers must take appropriate steps to ensure that their clients’ information appropriately is safeguarded. Appropriate communication with the client also is necessary ABA Model Rule 1.6.

AI and the Duty of Supervise and Unauthorized Practice of Law Under ABA Rule 5.1 and 5.3

SQUIRE PATTON BOGGS

- Under ABA Model Rules 5.1 and 5.3, lawyers have an ethical obligation to supervise lawyers and nonlawyers who are assisting lawyers in the provision of legal services to ensure that their conduct complies with the Rules of Professional Conduct.
- In 2012, the title of Model Rule 5.3 was changed from “Responsibilities Regarding Nonlawyer Assistants” to “Responsibilities Regarding Nonlawyer Assistance.” The change clarified that the scope of Rule 5.3 encompasses nonlawyers whether human or not.
- Under Rules 5.1 and 5.3, lawyers are obligated to supervise the work of the AI utilized in the provision of legal services, and understand the technology well enough to ensure compliance with the lawyer’s ethical duties.
- This includes making sure that the work product produced by AI is accurate and complete and does not create a risk of disclosing client confidential information.

Takeaway

SQUIRE PATTON BOGGS

Automated decisions based on black box algorithms can have legal, compliance and reputational consequences.

Understand how the AI data is gathered, sampled and used

Hold AI vendors accountable

Train your people and not just your AI

Establish AI policies and practices – ethics and norms

Keep abreast of changing landscape related to AI law

Additional Resources

SQUIRE PATTON BOGGS

Black Box AI and Bias

- *Weapons of Math Destruction* by Cathy O'Neil
- *How Vector Space Mathematics Reveals the Hidden Sexism in Language*, https://www.technologyreview.com/s/602025/how-vector-space-mathematics-reveals-the-hidden-sexism-in-language/
- *Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings*, https://arxiv.org/abs/1607.06520
- *How Do Machine Learning Algorithms Learn Bias?* https://towardsdatascience.com/how-do-machine-learning-algorithms-learn-bias-555809a1decb
  - Machine Learning Bias Caused By Source Data
  - Human Bias

Additional Resources

SQUIRE PATTON BOGGS

Other Examples of AI Bias

- Google's first generation of visual AI identified African Americans as gorillas.
- Voice command software in cars struggled to understand female voices
- NLP fails to recognize African-American vernacular English
- Microsoft's Tay.AI trained on twitter feeds produced racists and sexist tweets in under 24 hours

Additional Resources

SQUIRE PATTON BOGGS

- **AI Policies**
- The technology industry is grappling with creating a code of AI ethics
  - **FATE: Fairness, Accountability, Transparency, and Ethics in AI**, https://www.microsoft.com/en-us/research/group/fate/
  - **AI at Google: our principles**, https://www.blog.google/technology/ai/ai-principles/
  - **IEEE's Ethically Aligned Design**, https://ethicsinaction.ieee.org/
  - **ACM and AAAI's Conference on AI, Ethics, and Society**, https://sigai.acm.org/aimatters/blog/2017/09/20/new-conference-aaaiacm-conference-on-ai-ethics-and-society/
  - **ITI AI Policy Principles**, https://www.itic.org/dotAsset/50ed66d5-404d-40bb-a8ae-9eeeef55aa76.pdf

About the Speakers

Katharine Liao

Partner

Squire Patton Boggs, New York, katharine.liao@squirepb.com

Mrs. Liao represents employers in the retail, entertainment, technology and healthcare industries in all aspects of employment-related litigation before federal and state courts and administrative agencies. Resident in the firm's New York office, her practice is global with a particular emphasis and extensive experience with California and New York wage and hour class action litigation.

Stephanie Niehaus

Partner

Squire Patton Boggs, New York, stephanie.niehaus@squirepb.com

Ms. Niehaus is a litigator who represents clients in complex disputes in state and federal courts and in alternative forums throughout the US, and provides strategic advice to clients seeking to avoid or minimize the risk of litigation. She is experienced in advising and defending clients in a wide range of complex commercial matters across multiple industries, including chemicals, oil and gas, manufacturing, insurance, and financial services. She has particularly deep experience in matters involving toxic tort and product liability issues.

About the Speakers

Huu Nguyen

Partner

Squire Patton Boggs, New York, huu.nguyen@squirepb.com

Mr. Nguyen is a deal lawyer, focusing his practice on commercial and corporate transactions in the technology space. He counsels and assists clients with artificial intelligence arrangements, complex commercial arrangements, strategic relationships, financial regulatory matters, privacy and security matters, licensing, outsourcing, cyber law, intellectual property rights and general technology issues. Mr. Nguyen is a vice-chair of the ABA's committee on Artificial Intelligence and Robotics (2018-2019). He is also co-editor of the Thomson Reuter's Fintech Law Report. Prior to being an attorney, Huu was an AI programmer, and research scientist.

Global Coverage

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Budapest
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Doha
Dubai
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Moscow
Newark
New York
Northern Virginia
Palo Alto
Paris
Perth
Phoenix
Prague
Riyadh
San Francisco
Santo Domingo
Seoul
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC
West Palm Beach

Africa
Argentina
Brazil
Chile
Colombia
Cuba
India
Israel
Italy
Mexico
Panamá
Peru
Turkey
Ukraine
Venezuela

Office locations
Regional desks and strategic alliances