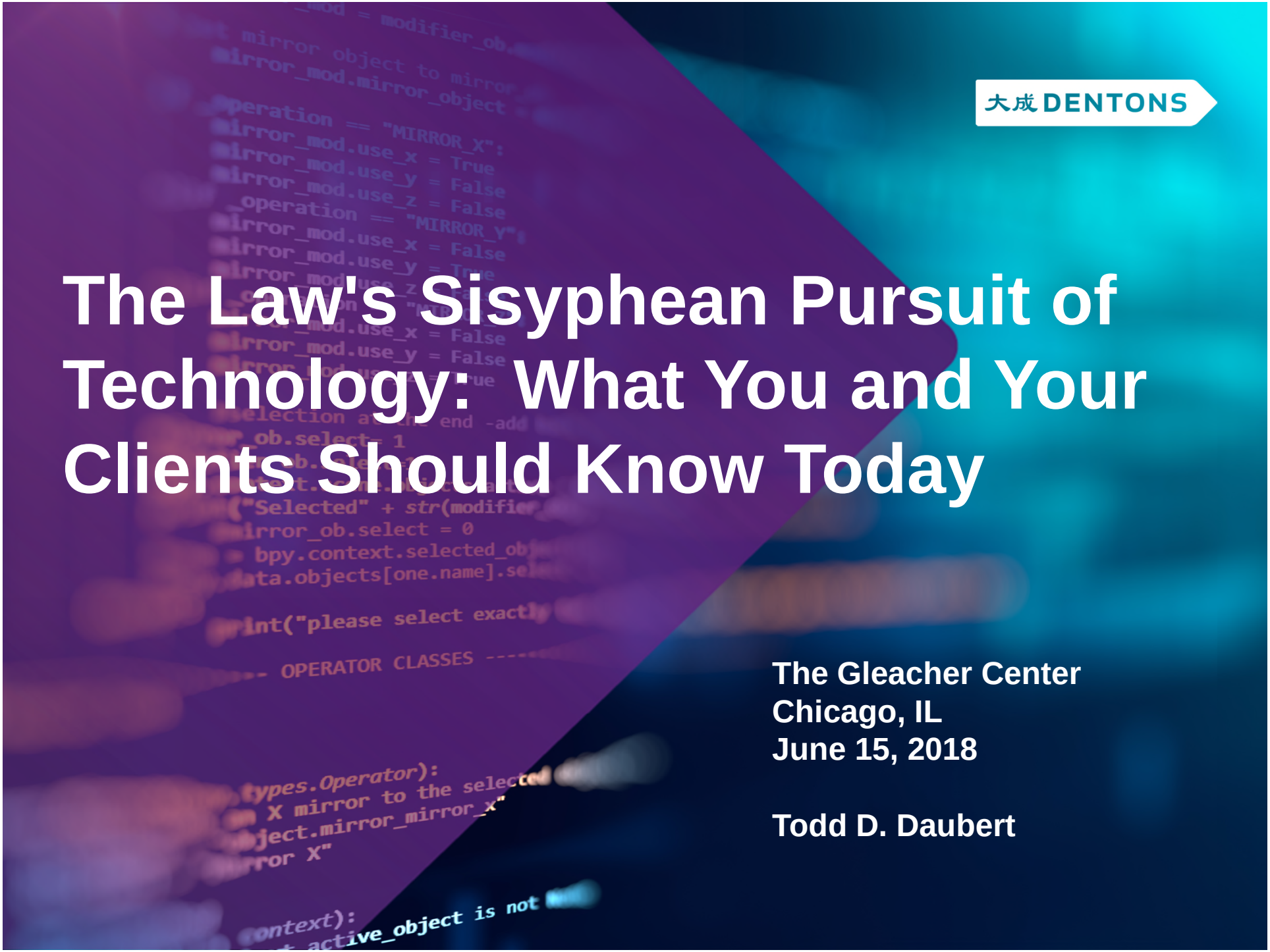


The Law's Sisyphean Pursuit of Technology: What You and Your Clients Should Know Today

The Gleacher Center
Chicago, IL
June 15, 2018

Todd D. Daubert

Agenda

- Privacy and Data Security
- Net Neutrality
- Robocalling, Spam and How it Will Impact Marketing
- Artificial Intelligence and Automation
- Deployment of 5G Services and the Growing Need for Spectrum

Privacy and Data Security

Privacy and Data Security

Growing Risks and Opportunities

As businesses become more reliant on technology, the importance of strong privacy and data security practices continues to grow.

The Risks:

- Breaches in 2017: 179 million records exposed, 1,570 breaches, with 91.3% occurring in the business section. [1]
- In 2017, the average company costs per data breach are $3.62 million (or $141 for each record breached), with the likelihood of a recurring material data breach over the next two years being 27.7%. [2]

The Opportunities:

- Strong privacy and data security practices and policies can lead to higher revenues and market valuations by:
  - being a material market differentiator;
  - increasing customer trust and loyalty; and
  - increasing the usability and value of the collected data.

Data security is essential for privacy, so it is difficult to discuss privacy without also discussing data security.

[1] 2017 Cost of Data Breach: Global Overview, Ponemon Institute, June 2017;
[2] Annual number of data breaches and exposed records in the United States from 2005 to 2017 (in millions), Statista, 2018.

Privacy and Data Security

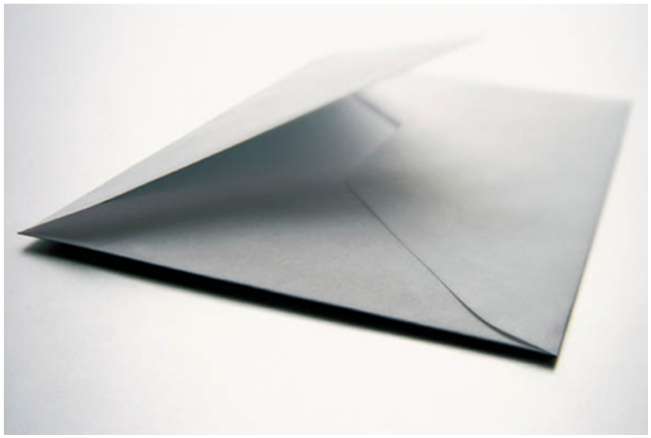
Differences in Regional Approaches: Lost in Translation

- US Data Privacy
  - Targeted, permissive
- European Data Privacy
  - Comprehensive, regulatory
- Canadian Data Privacy
  - A blend of the EU and US approaches -- more comprehensive (and cohesive) than the United States, but more business friendly than the EU
- Asia Pacific Data Privacy
  - Less mature, mixed approaches, but quickly developing

Privacy and Data Security: The US Approach

- Privacy is Judicially Created Under Other Constitutional Rights
  - No Explicit Right to Privacy in Constitution
    - "Zones of Privacy" under Penumbra of 1st, 3rd, 4th, 5th and 9th Amendments
  - Selective Sector-Based Approach
    - Healthcare
    - Finance
    - Children
  - Free Speech Almost Always Trumps Privacy

Society in the United States, as reflected in the law, has traditionally focused on expectations of privacy



Our traditions have heavily influenced our views of the appropriate use of technologies

Privacy and Data Security

The Patchwork in the United States

In the United States, hundreds of federal and state statutes and regulations have created a high duty of care for companies that collect, process, store, or handle personal information, depending on the type of data and the type of activity:

Federal laws

Privacy Act (5 U.S.C. § 552a)
CISA, Pub. L. No. 114-113, 129 Stat. 2242 (12/18/2015)
TCPA (47 U.S.C. § 227)
HIPAA (42 U.S.C. § 1320d-2(d))
FISMA (44 U.S.C. § 3551-58)

State Laws

Data breach notification laws
Other Privacy Laws (*e.g.*, CIPA (Pub. L. 106-554) and MRPA)

Many countries have higher standards than the US – with higher penalties. Transfer of data among jurisdictions can raise many issues. For instance, in the European Union, privacy is viewed differently, as a fundamental human right (now governed by the General Data Protection Regulation ("GDPR"), ("Regulation 2016/679")).

Privacy and Data Security

Changing Landscape of Data Security Regulation in the United States

- Consumer Privacy Protection Act of 2017 (H.R. 4081) - Introduced to Congress in October 2017 - would require certain commercial entities to implement a comprehensive consumer privacy and data security program.

- Last year, new privacy bills were proposed in 17 states — including New York, (A 7191 and S5603) and Massachusetts (HB 3698 and S 2062).[1]

- California's Consumer Privacy Act of 2018: A proposed ballot measure that would require businesses to inform consumers of data collation and sales activities, and offer clear opt-in or opt-out choices; this may appear on the November 2018 ballot.[2]

[1] Status of Internet Privacy Legislation By State, American Civil Liberties Union, 2018; [2] https://www.caprivacy.org/

Privacy and Data Security: The European Approach

- EU – Privacy is a Fundamental Human Right
  - Embodied in Article 8 of European Convention on Human Rights
  - Comprehensive Approach
  - Privacy Right Equal to Free Speech
  - Considered a Moral Issue

Privacy and Data Security: The Canadian Approach

- Privacy is not part of constitution, but broad statutory approach is taken
  - National Law (PIPEDA) governs collection, use, and disclosure of personal information.
    - Similar provincial laws also apply
- Individuals have rights similar to those in Europe
  - Accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; challenging compliance
- Sector-specific legislation such as the federal Bank Act further covers certain sensitive information

Privacy and Data Security: The Asia-Pacific Approach

- Multiple International Frameworks
  - APEC: Asia-Pacific Economic Cooperation
  - ASEAN: Association of Southeast Asian Nations
  - APPA: Asia Pacific Privacy Authorities
- National Legislation: Mix of broad EU-style and US-style approaches
  - PRC Network Security Law (or, the China Cybersecurity Law (CCL)) - Major reform to data management and internet usage regulations in China, and imposes new requirements for network and system security. Effective June 1, 2017.
  - Australia, Hong Kong, Japan and New Zealand have comprehensive privacy laws
  - Korea's laws regulate only certain industries
  - Taiwan's law regulates computer-processed data
- Data Breach Notification Requirements Applicable in Some Countries
  - Australia Notifiable Data Breach Scheme (NBS) - If an entity becomes aware there is reasonable grounds to believe there has been an eligible data breach impacted individuals and government must be notified. Effective February 22, 2018.

Privacy and Data Security

Global Struggles: Trade Wars, Protecting Critical Infrastructure, or both?

- Cross-border data transfer has become a prominent feature of global business, prompting new rules governing data storage and access.

- Growing faster than international trade or financial flows, the volume of global data flows grew 45-fold from 2005 to 2014.[1]

- Barriers to digital trade: high tariffs, localization requirements, cross border data flow limitations, intellectual property rights (IPR) infringement, forced technology transfer, web filtering, and cybercrime exposure or state-directed theft of trade secrets. [1]

- The renegotiation of the North American Free Trade Agreement (NAFTA) and the potential Trade in Services Agreement (TiSA) could address digital trade barriers to varying degrees. [1][2]

- [1] Digital Trade and U.S. Trade Policy, EveryCRSReport.com, May 2018; [2] Trade in Services Agreement (TiSA), European Commission, July 2017.

Privacy and Data Security

GDPR Basics

The GDPR replaced the Data Protection Directive 95/46/EC ("Directive 95/46/EC") on May 25, 2018.

The GDPR applies to all companies processing the personal data of EU data subjects, regardless of the company's location.

The GDPR applies to any organization that is:

- "established" in the EU and is processing "personal data" irrespective of whether the processing of personal data takes place within the EU or not; or
- not "established" in the EU, but which carries out the following processing activities:
  - The offering goods or services (even if no payment is required) to individuals in Europe; or
  - The monitoring of the behavior of individuals in Europe.

The so-called "equipment" test (under current law) is no longer applicable under the GDPR.

Privacy and Data Security

Organizations Established in the EU

Any organization that is established in the EU and processes the personal data of EU residents is subject to the GDPR.

- An organization is "established" in the EU through the "effective and real exercise of activity through stable arrangements" in the EU.
- The relevant factors to consider in determining whether an organization is “established in the EU” include whether the organization has:
    - a branch or subsidiary in the EU that acts on behalf of the company;
    - a local representative or agent.
- An organization processes "personal data" if it processes any direct or indirect information relating to an "identified" or "identifiable natural person" in EU.
    - "Indirect" identifiers include: location data, an online identifier, HR records, device IDs, IP addresses, cookies, and RFID tags.

Privacy and Data Security

Organizations that are NOT established in the EU

- An organization that is not established in the EU may nonetheless be subject to the GDPR if it both:
  - processes the personal data of EU residents; and either
  - offers goods or services (even if no payment is required) to individuals in Europe; or
  - monitors the behavior of individuals in Europe.
- Importantly, organizations that do not process any personal data of EU individuals would not be subject to the GDPR even if they process the personal data of non-EU individuals (*e.g.*, residents of the United States) using equipment physically located within the EU.

The storing and processing of US personal data in EU data centers would **not**, alone, trigger GDPR.

Privacy and Data Security

The Offering of Goods or Services to Individuals in the EU

The mere accessibility of a website from the EU or the use of a language generally used in the country where the organization is located would not trigger subject an organization to the GDPR.

By contrast, the use of a language or currency generally used in one or more EU member states combined with the possibility of ordering goods or services in that language would subject an organization to the GDPR.

The mentioning of customers or users who are in the EU in websites or advertisements could subject an organization to the GDPR.

For example, if a website is ”directed at” particular EU member states, the GDPR will apply.

Purchasing goods or services by EU residents outside EU alone would **not** trigger GDPR and mere accessibility of a website from EU, with cookies monitoring visitor activities, would generally **not** trigger GDPR.

Privacy and Data Security

The monitoring of individuals in the EU

The tracking of EU individuals for profiling purposes, particularly to make decisions concerning the individual, or for analyzing or predicting their personal preferences, behaviors and attitudes would subject an organization to the GDPR.

This monitoring and tracking can apply in the context of online behavioral advertising.

Privacy and Data Security

The Seven Principles of Processing of Personal Data

The controller is responsible for personal data processing that is:

- Lawful Fair and Transparent
- For Specified, Explicit and Legitimate Purposes (determined at the time of collection)
- Minimized
- Accurate
- As unidentifiable as possible
- Appropriately secure
- Accountable

Privacy and Data Security

Obligations of Organizations Subject to GDPR

Develop a EU-compliant privacy notice to provide detailed information to individuals about the processing of their personal data, specifying what data is processed, why it is processed, how it is processed (*i.e.*, what is done to the data and where it is processed or sent).

Exercise good data hygiene (ensure all data is accurate and up to date; unnecessary data is regularly purged; consent and opt-out requests are addressed; security measures in place).

Conduct a Privacy Impact Assessment to identify and minimize the risk of noncompliance.

Review and update the terms of vendor/processor agreements to be GDPR compliant.

Implement a breach notification procedure and breach log that includes (a) the nature of the breach; (b) the name and contact details of the Data Protection Officer (if applicable); (c) the likely consequences of the breach; (d) response and mitigation measures; and (e) reporting obligations.

Implement organizational measures to ensure compliance including (a) develop and implement a "subjects rights practice handbook" to describe policies and procedures that adheres to GDPR; (b) train employees to increase awareness and proficiencies on GDPR; (c) appoint a data protection officer (if appropriate); (d) and implement measures that meet the principles of data protection by design and data protection by default (which include data minimization and pseudonymization).

Determine whether a data protection officer is needed.

Net Neutrality

Net Neutrality

Impact on Business

- Two related issues are the focus of the Net Neutrality debates
  - Rules prohibiting blocking, throttling, and paid prioritization
  - Title I (information service) vs. Title II (telecommunications service) regulation
- The potential impact of Net Neutrality regulations on a company varies based on the role of the company in Internet ecosystem and its market power
  - Strict rules inhibit ISPs' ability to increase revenues by imposing access charges and offering innovative services that leverage their control of the network while lax rules subject edge providers and Main Street businesses to increased costs for reaching their customers
  - Established edge providers have the capital to negotiate and pay access charges to solidify dominance in the content market while new and would-be entrants may lack bargaining power and capital to pay for prioritization or compete with ISPs' vertically integrated services

Net Neutrality

History of Regulation

Net Neutrality

Current Debate

- Appellate Review
  - The D.C. Circuit will hear challenges to the 2017 *Restoring Internet Freedom Order* (filed by 23 States, edge providers, and public interest groups)
  - Seven Petitions for Certiorari to review the D.C. Circuit's 2016 decision upholding the *Title II Order* are currently pending before the Supreme Court (filed by major ISP trade associations, AT&T and a D.C.-based think tank).
- Congressional Review Act
  - Resolution to repeal the 2017 *Restoring Internet Freedom Order* and restore the 2015 rules passed the Senate 52-47.
  - Awaiting a vote in the House.
- State Legislation
  - Passed in Washington and Oregon; bills introduced in 22 other states.
  - The *Restoring Internet Freedom Order* preempts states from adopting ISP-specific regulations that are more restrictive than the rules adopted in the order but does not affect generally applicable laws that apply to ISPs

Net Neutrality

What's Really At Stake

- ISPs have said publicly that they will abide by net neutrality principles and support reasonable rules. In the short term, there is little risk an ISP would engage in blocking, throttling, or paid prioritization and risk public backlash or jeopardize good faith in Congress.
- Constant back and forth between FCC classifications and regulatory schemes creates uncertainty for consumers and companies.
- The eventual regulatory scheme will likely have a noticeable effect on the future of heavily broadband-reliant services.
  - Streaming video: 71% of Internet users use an OTT service [1]; by 2021 ~200 Million US consumers will use an OTT service or connected TV [2]
  - Cloud services: 20%of enterprises plan to more than double public cloud spend in 2018, and 71% will grow public cloud spend more than 20%.

[1] eMarketer, July 2017, “Programmatic Connected TV And OTT Video Advertising: Automation, Audience Attracts Digital And TV Ad Buyers.”

[2] Video Advertising Bureau, March 2018, "You Down with OTT: An Overview of the Competitive Video Ecosystem: 1Q '18 Report."

[3] Rightscale, February 2018, "State of the Cloud Report."

Robocalling, Spam and How It Will Impact Marketing

Robocalling, Spam and how it will impact marketing

Impact on Business

- Businesses with a legitimate interest in reaching consumers, for marketing or other reasons, should be able to reach them to promote their businesses and relay useful information.
  - Litigation risk is creating a chilling effect on legitimate businesses and keeping consumers from fielding calls.
  - Uncertainty around what equipment is prohibited means businesses must constantly reconfigure their sales strategies
- Policy should balance protecting legitimate businesses with weeding out bad actors to protect consumers:
  - Thorough vetting of blocking and call authentication protocols;
  - Clear guidance from the FCC; and
  - Consistent application of the law by the courts.

Robocalling, Spam and how it will impact marketing

Regulatory Challenges and Relevant Legal Issues

- "Autodialer" uncertainty
  - In *ACA International v. FCC*, the D.C. Circuit set aside the FCC's interpretation of what constitutes an automatic telephone dialing system.
  - The FCC must now revisit how it what functions a device must be able to perform in order to be considered an autodialer and what constitutes the "capacity" to perform such functions.
- Reassigned Numbers
  - The D.C. Circuit also instructed the FCC to revisit how to interpret whether a caller has received a "called party" prior express consent for calls to reassigned numbers.
- Revocation of consent
  - What opt-out methods are sufficiently clearly defined to satisfy the D.C. Circuit's instruction to make revocation possible through any reasonable means clearly expressing a desire to no longer receive messages?

Robocalling, Spam and how it will impact marketing

Latest developments

- Call Blocking
  - November 2017 *Order* permits voice providers to proactively block categories of calls that are invalid, unallocated, unused, or on a Do-Not-Originate list.
  - Related *FNPRM* seeks comment on potential challenge mechanism to ensure erroneously blocked numbers can be unblocked.
- Reassigned Numbers
  - The FCC has proposed to ensure databases are available to allow callers to lookup when a number has been reassigned; weighing whether to establish a single database, reporting requirement, and safe harbor
  - As an alternative, the agency has sought comment on whether to require, or allow voluntary reporting to, commercial data aggregators.
- Call Authentication
  - The FCC has accepted the North American Numbering Council's recommendations for implementing the SHAKEN/STIR framework to eliminated spoofed unwanted calls.

Artificial Intelligence (AI) / Automation

Artificial Intelligence (AI)

I am in the camp that is concerned about super intelligence. - **Bill Gates**

I think it's too early to think about monitoring mechanisms. It's more important right now to build a consensus in the industry and academia around what are the things that would have a chilling effect. - **Skype Co-Founder Jaan Tallinn**

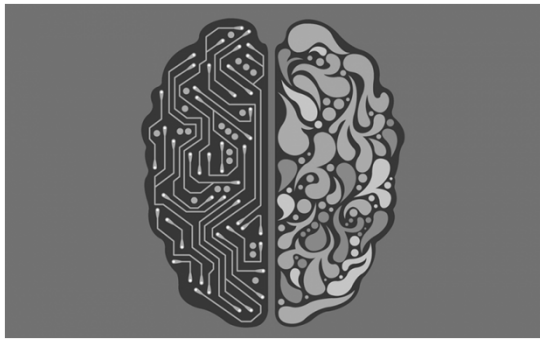
I agree that the future is scary and very bad for people. If we build these devices to take care of everything for us, eventually they'll think faster than us and they'll get rid of the slow humans to run companies more efficiently. - **Steve Wozniak, Apple co-founder**

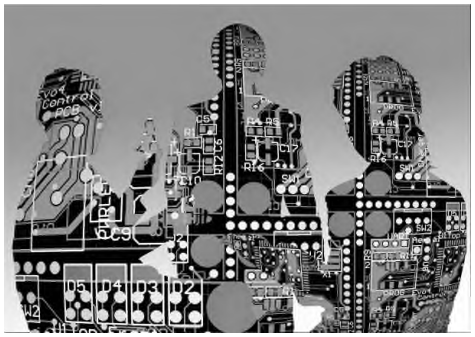
I think we should be very careful about artificial intelligence. If I had to guess at what our biggest existential threat is, it's probably that. - **Elon Musk**

In short, the rise of powerful AI will either be the best, or the worst thing, ever to happen to humanity. We do not yet know which. - **Stephen Hawking**

Artificial Intelligence (AI) - What Is It?

- **First Defined in 1950's** "Ever aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it." - Professor John McCarthy Dartmouth College (1956)
- **Artificial Intelligence** is the development and advancement of intelligence machine and computer systems that are capable of performing tasks that previously required human intelligence.
- **Machine learning** generally entails teaching a machine how to do a particular task, like recognizing a number, by feeding it data and directing it to make predictions on that data. Machine learning is becoming easier to implement, but often requires an engineer to help program.
- **Deep learning** is a type of machine learning that does not require an engineer. It often involves artificial neural networks - a mathematical system inspired by the way neurons work together in the human brain.

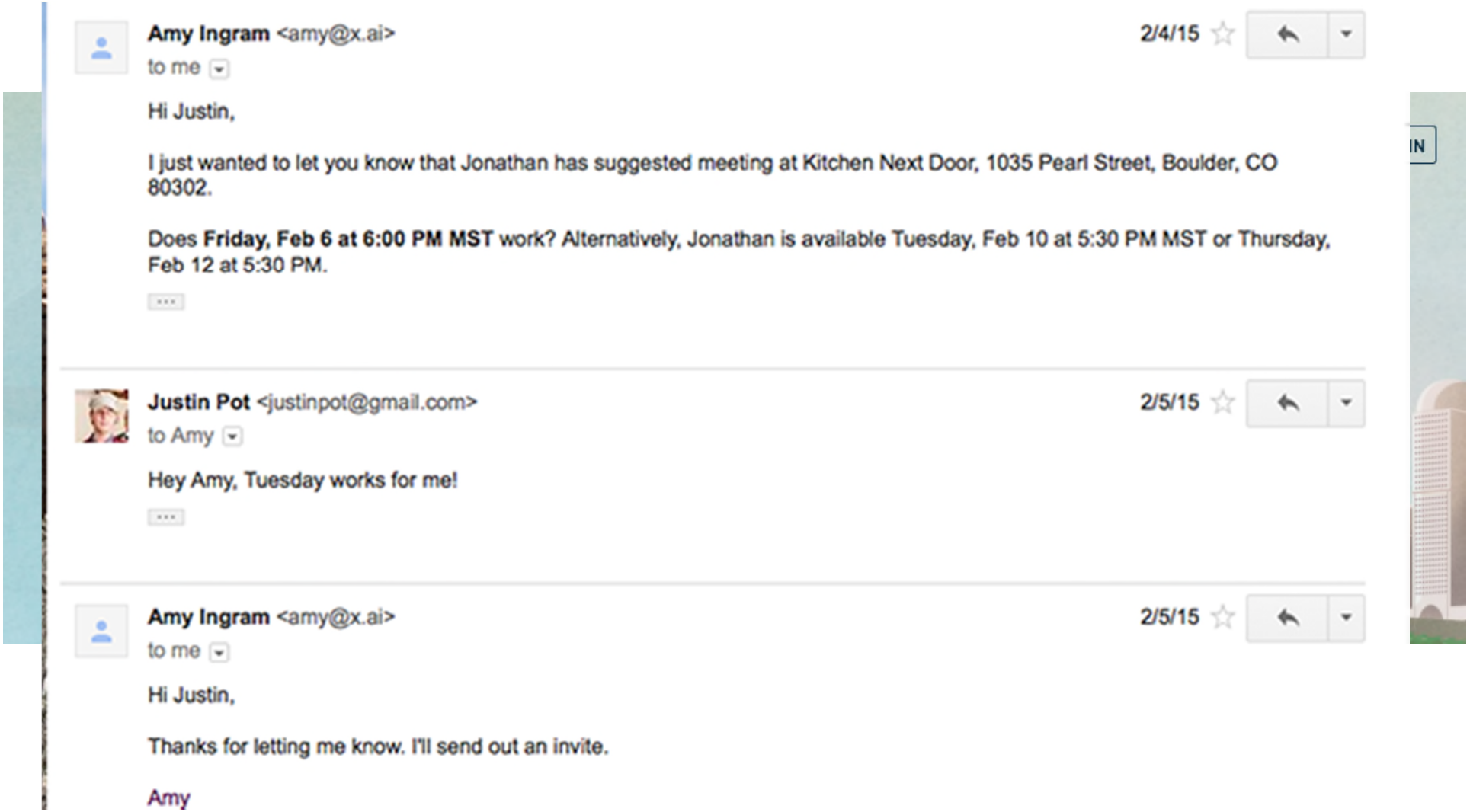




Artificial Intelligence (AI) - Trends

- Automated transportation
- Cyborg technology
- Taking over dangerous jobs
- Workforce developments (HR, hiring)
- Personal assistants
- Big data analytics
- Legislation
- Solving complex public issues

AI Assistants



Amy Ingram <amy@x.ai> 2/4/15

to me

Hi Justin,

I just wanted to let you know that Jonathan has suggested meeting at Kitchen Next Door, 1035 Pearl Street, Boulder, CO 80302.

Does **Friday, Feb 6 at 6:00 PM MST** work? Alternatively, Jonathan is available Tuesday, Feb 10 at 5:30 PM MST or Thursday, Feb 12 at 5:30 PM.

Justin Pot <justinpot@gmail.com> 2/5/15

to Amy

Hey Amy, Tuesday works for me!

Amy Ingram <amy@x.ai> 2/5/15

to me

Hi Justin,

Thanks for letting me know. I'll send out an invite.

Amy

Artificial Intelligence (AI) - Legal Trends

- International trends
  - France, European Union, South Korea
- US Trends
  - Elon Musk - governors should regulate AI "before it's too late."
  - Should AI be subject to the same laws as its human operator or treated under a product liability framework?
  - Discrimination concerns
    - Stony Brook University released an app that could guess the ethnicity of a person to over 80% accuracy based on name

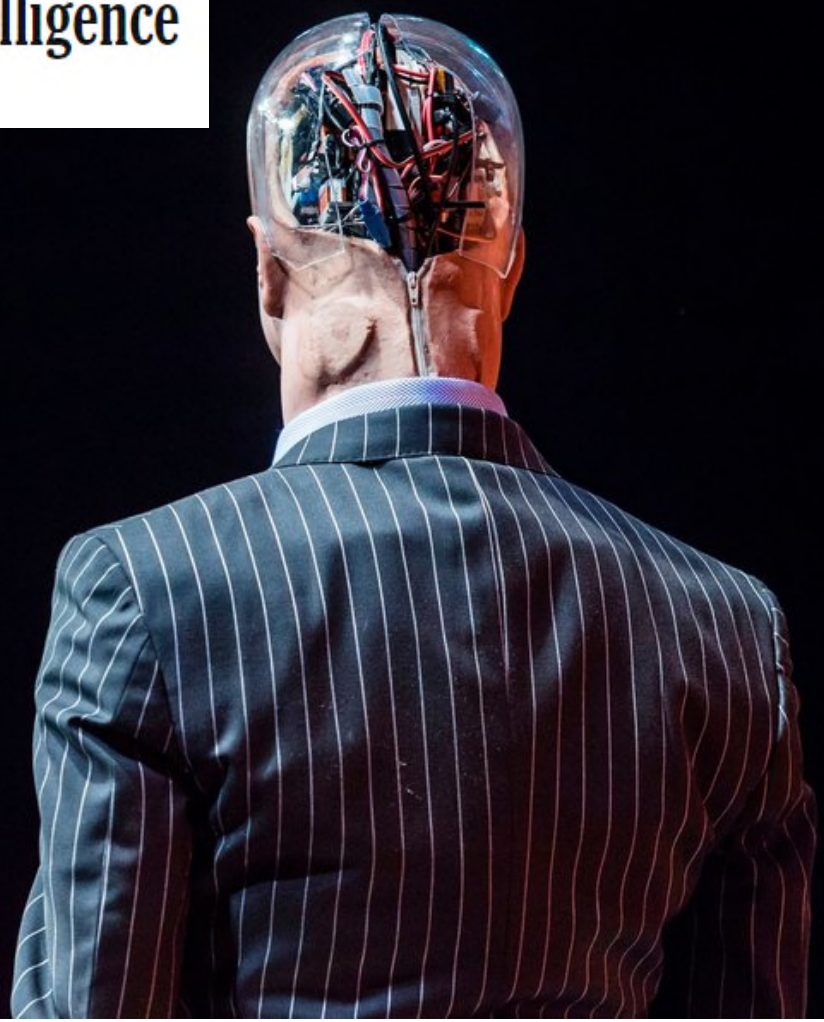
Artificial Intelligence - Legal Trends

OP-ED CONTRIBUTOR

How to Regulate Artificial Intelligence

By Oren Etzioni

1. Treat like humans
2. Disclose robot existence
3. Express consent



Artificial Intelligence (AI) - Takeaways

AI is in its inception. Rapid changes will be seen in the next years.

Regulating AI raises critical legal and ethical questions.

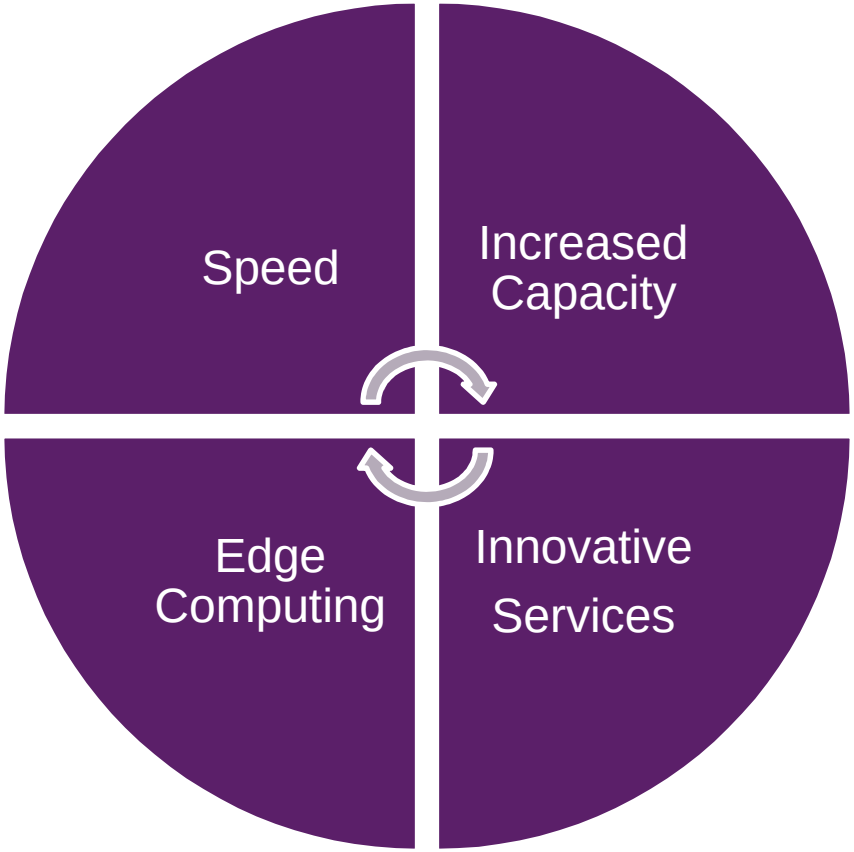
AI presents tremendous benefits, but significant challenges.

Companies need to balance AI benefits with future regulatory changes.

Deployment of 5G Services and Growing Need for Spectrum

5G Deployment and the Growing Need for Spectrum

Impact on Business



5G Deployment and the Growing Need for Spectrum

Legal Challenges for Deployment

- Spectrum
  - High band spectrum required for infrastructure investment--28 GHz auction scheduled for November 14, 2018; 24 GHz auction to follow
  - Mid-band spectrum in the 3.5GHz band the subject of ongoing CBRS proceeding; up to 150 MHz may be up for grabs
- Permits
  - Local officials control much of the 5G deployment process through permitting for tower siting, rights of away, and pole attachments.
  - Cooperation, coordination, and policies for leveraging existing towers and facilities can cut red tape.
- Backhaul
  - Small cell connections to cable/fiber backhaul are necessary to support wireless densification and realize potential of 5G.
  - Efficient deployment and utilization will require cooperation among carriers and building owners and local regulators.

5G Deployment and the Growing Need for Spectrum

What to Expect

- Standards
  - In December 2017 3GPP announced 5G NR, the first global standard of what 5G will look like
  - Trials underway for networks and equipment built to 5G NR specifications
- Global competition
  - China's Huawei is signing Memorandums of Understanding with telcos across Europe and Asia to run trials for 5G equipment, signaling the potential for potential deals and making China an early front runner in the race for 5G.
  - The US has acknowledged the threat coming from China--blocking the proposed merger of Broadcom and Qualcomm as a result and urging AT&T to cut ties with Huawei.

Thank you

Dentons US LLP
233 South Wacker Drive
Suite 5900
Chicago, IL 60606-6404
United States

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work. www.dentons.com.