Big Data & Law

AzALL-SANDALL Symposium on Digital Dilemmas
Feb. 16, 2018

Gary E. Marchant, J.D., Ph.D.
Gary.marchant@asu.edu
“[P]oliticians – and judges for that matter – should be wary of the assumption that the future will be little more than an extension of things as they are.”

- from Jeffrey Rosen, Roberts v. The Future, NY Times, Aug. 28, 2005
Technology Revolutions of the 20th Century
Technology Adoption Rates Acceleration

Consumption spreads faster today

Source: Charlie Catlett, Argonne Nat'l Laboratory
Ray Kurzweil: The Law of Accelerating Returns

“An analysis of the history of technology shows that technological change is exponential, contrary to the common-sense ‘intuitive linear’ view. So we won’t experience 100 years of progress in the 21st century – it will be more like 20,000 years of progress (at today’s rate).”
Regulating the internet giants

The world’s most valuable resource is no longer oil, but data

“Every two days we create as much information as we did from the dawn of civilization up until 2003.”

Eric Schmidt, CEO, Google

“...growing at 50 percent a year...”

“... data a new class of economic asset, like currency or gold.”
Four Characteristics of Big Data

1. Cost efficiently processing the growing **Volume**
   - 2010: 1 ZB
   - 2020: 35 ZB (50x growth)

2. Responding to the increasing **Velocity**
   - 30 Billion RFID sensors and counting

3. Collectively Analyzing the broadening **Variety**
   - 80% of the world's data is unstructured

4. Establishing the **Veracity** of big data sources

**1 in 3** business leaders don’t trust the information they use to make decisions

Source: IBM
Some Technologies
Social Media

BIG DATA
GPS Evidence

- Police tracking of suspect location
  - GPS device
  - Cell phone
- Digital stalkers
- Divorce attorney tracking of spouses
- Monitoring of employees
- Sex offenders
- Bank robber
- Speed limit enforcement/defense
- GPS cameras ("geotagging")
Artificial Intelligence/Machine Learning
AI: Machine Learning

### Human Computer Programming

- Machine mechanically implements human-made code
- Bad outcomes are attributable to bad code by human programmer
- Human programmer can explain why machine did what it did

### Machine Learning

- Humans provide data and specify overall goal for machine
- Machine self-learns and adapts its approach to maximize specified goal
- Limited explanation for why machine did what it did
Internet of Things
IoT Devices Outnumber Humans on Earth

By 2025 there will be ~8 connected devices per human on earth

- IoT Devices
- Humans

Projections in Billions
Sources: Our World in Data, Statista
RFID – Current Applications

- Inventory control
- School tracking
- Gasoline quick-pay
- Employee location monitoring
- Hospital patient monitoring
- Identification of pets
- Livestock tracking
- Windshield-mounted toll and entry tags
- Amusement parks (e.g., Leggo Land)
- Libraries track books
- Document tracking
- RFID chips in US passports
- Credit cards
- Airline luggage tracking
- Tracking underground miner location
Blockchain

What it means for clients, contracts—and law practice

Financial services
Government services
Healthcare
Energy markets
Supply chains
Smart things
World trade
Biometrics
Brain Scanning

Potential legal applications include:
- Lie detection
- Terrorist identification
- Latent racial animus
- Competency
- Propensity for violence
- Recidivism risk
- Pain
- Drug and alcohol use
- Awareness in vegetative state
Genetic Surveillance

- We are constantly shedding our DNA in saliva, hair, skin cells
- New techniques allows collection, amplification, and characterization of our DNA
- Examples:
  - Cigarette butt
  - Chewing gum
  - Drinking glass
  - Straw
  - Envelope

ABA Journal, August 2011
Congressional inquiry responses released: Data brokers refuse to name sources

*Summary:* A Congressional inquiry told nine major data brokerage companies to explain how they collect and sell consumer information. The data dealers have responded with PR and generalities.
Some Applications
A first: biometrics used to sentence criminal

A judge ruled that biometric facial recognition could be submitted as evidence marking the first time such evidence has been used in a criminal trial; this move surprised many legal and scientific experts as facial recognition technology does not follow basic legal standards required for evidence; the decision may or not become a legal precedent as it was not made by a California appellate or supreme court.

In early January, convicted murder Charles Heard received twenty-five years to life in a California prison for murder.

The case was unique because it was the first time that biometric facial recognition technology had been permitted to be used as evidence in the court room.
Image of suspect in school aide's 1992 slaying generated from his DNA

By Crimesider Staff AP September 29, 2016, 10:42 AM

U.S. soldiers are revealing sensitive and dangerous information by jogging

A portion of the Strava Labs heat map from Kandahar Airfield in Afghanistan, made by tracking activities. (Screenshot)

By Liz Sly  January 26 at 4:00 PM
When Fitbit Is the Expert Witness

An upcoming court case will use fitness-tracking data to try and prove a plaintiff’s claim, bringing us one step closer to the new age of quantified self-incrimination.

Self-tracking using a wearable device can be fascinating. It can drive you to exercise more, make you reflect on how much (or little) you sleep, and help you detect patterns in your mood over time. But something else is happening when you use a wearable device, something that is less immediately apparent: You are
A cheating US husband has been charged with killing his wife after police said data from her wearable fitness tracker contradicted his version of events.

Richard Dabate, 40, claimed to have seen Connie Dabate shot to death more than an hour before her Fitbit device recorded her last movements.

He told detectives that she was killed by a home intruder in the US state of Connecticut on 23 December 2015.

But police say her electronic device tells a different story.

Mr Dabate was charged this month with murder, tampering with physical evidence and making false statements about his 39-year-old wife’s death.
Amazon Alexa May Be a Witness to Murder

By JILL BLEED, ASSOCIATED PRESS
LITTLE ROCK, Ark. — Dec 28, 2016, 4:53 PM ET

FILE - This July 29, 2015, file photo shows Amazon’s Echo speaker, which responds to voice commands, in New York. A prosecutor investigating the death of a man who...
Cops use pacemaker data to charge homeowner with arson, insurance fraud

Police called pacemaker data an 'excellent investigative tool' that provided 'key pieces of evidence' to charge a man with arson and insurance fraud.

If you are dependent upon an embedded medical device, should the device that helps keep you alive also be allowed to incriminate you in a crime? After all, the Fifth Amendment of the U.S. Constitution protects a person from being forced to
“We know now that many of the devices participating in the attack were IoT devices such as smart refrigerators, thermostats, and toasters.”

Distributed denial of service (DDoS) attacks are a common problem for network administrators around the world. Websites small and large get targeted by them every day. But this Friday, dozens of major websites were affected by a widespread attack — and this time the Internet of Things is in the spotlight.

Friday's attack — already referred to as the October 2016 Dyn Cyberattack, showing immediately that we need snappier names for these events — affected many popular websites including Twitter, Amazon, Reddit, Netflix, and more. These websites shared one thing in common: they all used a common domain name system (DNS) provider, Dyn.

From about 0930 ET until just after 1800 ET, Dyn’s servers were attacked in three DDoS waves. We know now that many of the devices participating in the attack were IoT devices such as smart refrigerators, thermostats, and toasters. A group called “New World Hackers” has claimed responsibility for the attack.
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

just as you're parking in front of a ditch.
Hacking Into Smart Devices

Stranger hacks family's baby monitor and talks to child at night

By CHANTE OWENS  January 7, 2016

A family living in Washington is speaking out about the horrors they experienced while operating a baby monitor inside their 3-year-old son's bedroom. The couple Jay and Sarah were alarmed to discover that a stranger had hacked into their baby monitor and was spying on their toddler, sometimes speaking disturbing messages into the device, as CBS News describes.

https://www.youtube.com/watch?v=4akjYG-8yd8
New surveillance cameras will use computer eyes to find 'pre crimes' by detecting suspicious behaviour and calling for guards

- Computerised detectors look for 'abnormal' behaviour
- When suspicious individuals are seen, guards called
- BRS machines have been trialled in numerous locations
- 288 cameras to be installed on subway in San Francisco

By Rob Waugh

Published: 09:12 EDT, 5 June 2012 | Updated: 09:12 EDT, 5 June 2012

24

View comments

A new generation of computerised 'Big Brother' cameras are able to spot if you are a terrorist or a criminal - before you even commit a crime.

The devices are installed in places like train stations or public buildings where they scan passers by to see if they are acting suspiciously.

Using a range of in-built parameters of what is 'normal' the cameras then send a text message to a human guard to issue an alert - or call them.
https://www.youtube.com/watch?v=XH1wQEgROg4
A New Weapon in the Trial Lawyer’s Arsenal

By Quentin F. Urquhart, Jr. and John E. Swanson

Trial exhibits made by 3D-scanning technology have established a new standard for accurately documenting and displaying evidence.
Could Blockchain Evidence Be Inadmissible?

By Casey C. Sullivan, Esq. on May 5, 2016 12:04 PM

Blockchain technology creates a virtually incorruptible, dispersed database of all transactions in a network. It’s the technology that helped make Bitcoin a (relative) success, but it’s often hailed as a potentially transformative technology in finance, business, and the law. There are contracts that use the blockchain, for example. There may one day even be entire government databases based on blockchain technology.

But, as James Ching recently pointed out, there could be a downside to all the blockchain hype. It's possible that blockchain evidence may be inadmissible hearsay.
Digital Fabrication

DIGITAL MANIPULATION AND PHOTOGRAPHIC EVIDENCE: DEFRAUDING THE COURTS ONE THOUSAND WORDS AT A TIME

Zachariah B. Parry
'Robot lawyer' that overturned 160,000 parking tickets now helping refugees

Joshua Browder's DoNotPay is now helping refugees CREDIT: DONOTPAY

Hollywood's last true eccentric: the spectacularly odd life of American Gods star Crispin Glover
02 May 2017

Can you spot the snake in this picture?
26 Apr 2017

General election 2017: Polls and odds tracker
02 May 2017

Warning over fake bank websites targeting British savers
02 May 2017

Facebook could be used to find Madeleine McCann, expert says
27 Apr 2017
Facial Recognition Technology Used in Jury Consulting
Reading Faces in All the Wrong Places: Emotion Analytics Software in the Courtroom

From privacy concerns to juror distraction, these are the issues that arise from applying emotion analytics in the courtroom.

Rick Martinez, Legaltech News

January 7, 2016

Most people know Facebook and Google can “read” a face and identify the person. Next generation software goes much further: uncovering moods and emotions. Courts and trial counsel alike should consider now the implications of possible courtroom use.
Working Upstream: How Far Can You Go with Sewage-Based Drug Epidemiology?

Daniel A. Burgard,†‡ Caleb Banta-Green,‡ and Jennifer A. Field§

†Chemistry Department, University of Puget Sound, Tacoma Washington 98416, United States
‡Alcohol and Drug Abuse Institute, University of Washington, Seattle Washington 98105, United States
§Department of Environmental and Molecular Toxicology, Oregon State University, Corvallis Oregon 97331, United States

Analytes by 2–4 orders of magnitude. With these techniques, quantification of drugs at even the subpart per trillion range (ppt) is possible.

Jones-Lepp et al. reported the first detection of two drugs, methamphetamine (a pharmaceutical and illicitly manufactured drug) and methylenedioxymethamphetamine (MDMA, commonly referred to as ecstasy, an illicit drug) in the effluent of two wastewater treatment plants (WWTPs) in the U.S.² Interestingly, the idea of a community-scale surveillance tool using sewage was actually proposed three years earlier by Christian Daughton at the U.S. Environmental Protection Agency.³ The field received worldwide media attention when a press release from the Marine Nexus Institute for Pharmacological
Orbitz Worldwide Inc. has found that people who use Apple
hotels, so the online travel agency is starting to show them
different, and times costlier, options than Windows
visitors see.

The Orbitz effort, which is in its early stages, demonstrates
innocuous information—in this case, the fact that customers

Orbitz executives confirmed that the company is experimentally
rank results by price.

Orbitz found Mac users on average spend $20 to $30 more
given the site's average nightly hotel booking is around $100.
to book a four- or five-star hotel than PC users, Mr. Yee says.

Why the Apple Demographic Is So Important

Apple is practically creating its
own demographic, and...
Andrew Thomas’s life insurer knows exactly when he arrives at his local gym. The company is notified when he swipes his membership card, and 30 minutes later, it checks that he is still there, tracking his location through his smartphone.
Machine Testimony

ANDREA ROTH

ABSTRACT. Machines play increasingly crucial roles in establishing facts in legal disputes. Some machines convey information—the images of cameras, the measurements of thermometers, the opinions of expert systems. When a litigant offers a human assertion for its truth, the law subjects it to testimonial safeguards—such as impeachment and the hearsay rule—to give juries the context necessary to assess the source’s credibility. But the law on machine conveyance is confused: courts shoehorn them into existing rules by treating them as “hearsay,” as “real evidence,” or as “methods” underlying human expert opinions. These attempts have not been wholly unsuccessful, but they are intellectually incoherent and fail to fully empower juries to assess machine credibility. This Article seeks to resolve this confusion and offer a coherent framework for conceptualizing and regulating machine evidence. First, it explains that some machine evidence, like human testimony, depends on the credibility of a source. Just as so-called “hearsay dangers” lurk in human assertions, “black box dangers”—human and machine errors causing a machine to be false by design, inarticulate, or analytically unsound—potentially lurk in machine conveyances. Second, it offers a taxonomy of machine evidence, explaining which types implicate credibility and how courts have attempted to regulate them through existing law. Third, it offers a new vision of testimonial safeguards for machines. It explores credibility testing in the form of front-end design, input, and operation protocols; pretrial disclosure and access rules; authentication and reliability rules; impeachment and courtroom testing mechanisms; jury instructions; and corroboration rules. And it explains why machine sources can be “witnesses” under the Sixth Amendment, refocusing the right of confrontation on meaningful impeachment. The Article concludes by suggesting how the decoupling of credibility testing from the prevailing courtroom-centered hearsay model could benefit the law of testimony more broadly.
SCIENTISTS WANT TO TAKE VIRTUAL REALITY TO COURT

JURORS MAY ONE DAY VISIT CRIME SCENES USING FORENSIC HOLODECKS

By Sarah Fecht  January 9, 2015

This virtual reality reenactment of the Tamir Rice incident shows the perspective of the officers as they drove toward the area where Rico was shot.
Court: Judges Can Consider Predictive Algorithms in Sentencing

By JOE PALAZZOLO
Jul 13, 2016 5:04 pm ET

Sentencing judges may take into account algorithms that score offenders based on their risk of committing future crimes, Wisconsin’s high court ruled on Wednesday.
Machine Testimony

ANDREA ROTH

ABSTRACT. Machines play increasingly crucial roles in establishing facts in legal disputes. Some machines convey information—the images of cameras, the measurements of thermometers, the opinions of expert systems. When a litigant offers a human assertion for its truth, the law subjects it to testimonial safeguards—such as impeachment and the hearsay rule—to give juries the context necessary to assess the source's credibility. But the law on machine conveyance is confused: courts shoehorn them into existing rules by treating them as "hearsay," as "real evidence," or as "methods" underlying human expert opinions. These attempts have not been wholly unsuccessful, but they are intellectually inconsistent and fail to fully empower juries to assess machine credibility. This Article seeks to resolve this confusion and offer a coherent framework for conceptualizing and regulating machine evidence. First, it explains that some machine evidence, like human testimony, depends on the credibility of a source. Just as so-called "hearsay dangers" lurk in human assertions, "black box dangers"—human and machine errors causing a machine to be false by design, miscalculate, or analytically unsound—potentially lurk in machine conveyances. Second, it offers a taxonomy of machine evidence, explaining which types implicate credibility and how courts have attempted to regulate them through existing law. Third, it offers a new vision of testimonial safeguards for machines. It explores credibility testing in the form of front-end design, input, and operation protocols; pretrial disclosure and access rules; authentication and reliability rules; impeachment and courtroom testing mechanisms; jury instructions; and corroboration rules. And it explains why machine sources can be "witnesses" under the Sixth Amendment, refocusing the right of confrontation on meaningful impeachment. The Article concludes by suggesting how the decoupling of credibility testing from the prevailing courtroom-centered hearsay model could benefit the law of testimony more broadly.
If that headline doesn’t make much sense, welcome to the 21st century when a program designed to automatically buy random items from illegal marketplaces can be arrested by Swiss police. As you’ll recall, Swiss police seized a program called Darknet Shopper, a bot that visited darknet markets and bought random items with bitcoin. Most of the items were mundane – counterfeit goods and the like – but the robot also ordered some ecstasy.
Case Outcome Prediction

AI Beats Human Lawyers in CaseCrunch Prediction Showdown + DATA UPDATES


artificiallawyer

October 28, 2017
Legal AI company **Voltaire** has launched an application that will allow lawyers and litigation consultants to rapidly analyse potential jurors by crunching public Big Data, including social media posts.
Judge Analytics

Understand how judges think, write, and rule.

Judge Dashboard
The Judge Dashboard encompasses your judge’s entire career — every decision, every citation, housed in a single location. The dashboard lets you identify the cases, circuits, and judges your judge finds most persuasive.

Specific Language
Uncover the rules and specific language your judge favors and commonly cites. Pinpoint distinctions that set your judge apart to ensure you never miss the nuance that could win or lose your argument.

Litigation Strategy
Make data-driven decisions about everything from how to frame arguments to whether to file a particular motion — decisions that can make or break a case.
Judge's Football Team Loses, Juvenile Senter Go Up

No, seriously.

EMILY DERUY | SEP 7, 2016 | EDUCATION
“THE BEST TECHNOLOGY MEANS FEWER ATTORNEYS NEEDED ON EACH CASE.”

RICHARD ROSENSWEIG
DIRECTOR, LITIGATION GROUP
GOULSTON & STORRS
BOSTON
Why Hire a Lawyer? Computers Are Cheaper

By JOE PALAZZOLO

When the roofs of three jet hangers in Virginia collapsed under heavy snow and crushed 14 private jets in 2010, the owner of the hangars prepared for the inevitable lawsuits.

Landow Aviation preserved about 8,000 gigabytes—the equivalent of about eight new desktop computers filled...
Machine Learning Saves JPMorgan Chase 360,000 Hours of Legal Work

By Casey C. Sullivan, Esq. on March 8, 2017 10:11 AM

Here's a sobering fact for lawyers: Last year, a machine learning program used by JPMorgan Chase saved the company 360,000 hours of work, work that would normally be performed by lawyers and loan officers.

That's more than 41 years worth of nonstop legal work -- all handled in a few seconds, by some well-designed software.

“A New Era of Automation”
AI and the Practice of Law

“Good News”
- Adoption of AI in practice of law will be evolutionary, not revolutionary
- Most lawyer functions will not be performed by AI in foreseeable future
- Adoption of AI offers opportunity to be leader in efficiency, cost savings, accuracy

“Bad News”
- AI will take over a steadily increasing share of law firm billable hours
- AI will require knowledge/abilities outside the existing skill set of most current practicing attorneys
- Incorporation of AI into practice will soon be a matter of keeping up rather than being a leader
Changes Coming?
A Supreme Court case this week could change US digital privacy standards

As the leaves fall, the high court mulls privacy in a time of change. (Reuters/Yuri Gripas)
EU General Data Protection Regulation
25 May 2018
Conclusion: Advice from “The Great One”

“I skate to where the puck is going to be, not where it has been.”

Wayne Gretzky