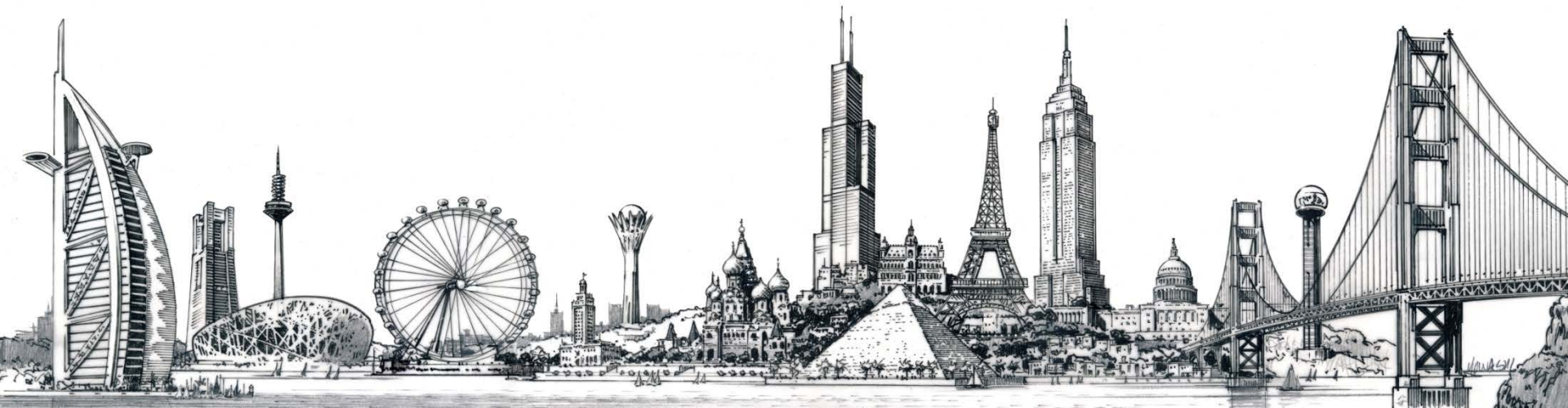
PRIVACY AND THE INTERNET OF THINGS

W. Reece Hirsch, CIPP
Co-head of Privacy and Cybersecurity Practice

Morgan Lewis

Morgan Lewis Breakfast Briefing
December 10, 2015



What is the Internet of Things?

- No agreed upon definition of the Internet of Things (IoT)
- Generally refers to a decentralized network of “smart objects.” Items that can
  - Sense, log, interpret and communicate information
  - Act on their own accord or in cooperation with other objects
- IoT raises new privacy questions that the law is only beginning to answer

Examples of IoT Devices

- Personal fitness monitors
- Smart kitchens
- Internet-connected televisions
- Self-driving cars
- Smart light bulbs
- Internet-connected surveillance cameras
- Sensor-driven, Wi-Fi enabled self-learning thermostats
- Wirelessly connected medical devices like insulin pumps and pacemakers
- “Smart grid” energy management technologies
- Internet-connected parking meters
- An egg tray that syncs with a smartphone to report how many eggs remain and when they are going bad
- Talking Barbie dolls

Ubiquitous Computing

- IoT is a network connecting computers and people

- Utilizing sensors that collect data and “actuators” – mechanical devices that move something
  - Embedded in physical objects that we use every day

- Trend toward a linking of the digital and physical worlds
  - Achieving “ubiquitous computing” where computers appear all around us and recede into the background of our lives
  - Google Glass
  - “Augmented reality”

- Growth of IoT represents a significant evolution of the Internet

By the Numbers

- Between 2008 and 2009, for the first time, the number of devices connected to the Internet became greater than the number of people in the world

- Mobile devices first outnumbered people in 2013

- Number of devices connected to the Internet worldwide is estimated to be 25 billion
  - Expected to reach 50 billion devices by 2020
  - Fastest growth is in the IoT sector

FTC Intends to Police IoT

- May 2015: FTC Commissioner Julie Brill declares that the FTC's enforcement powers extend to cover privacy and security risks posed by the IoT
  - Keynote address at the European Data Protection Days conference in Berlin
  - No specific privacy law that directly targets IoT data collection and security
  - FTC regulates IoT based on jurisdiction over unfair and deceptive trade practices under Section 5 of the FTC Act

- Section 5 doesn't specifically address application of privacy principles to cutting-edge technologies
  - Concepts of deception and unfairness may be interpreted to cause companies to examine
    - What they are telling consumers about data collection and use
    - What consumers understand about those practices

FTC Calls For Adoption of Best Practices

- "The two basic principles [embodied in Section 5] – don't deceive consumers by express representations or omissions, and don't harm them in ways that they cannot avoid – play an important role in addressing some of the biggest data protection challenges arising from the Internet of Things."
  – FTC Commissioner Julie Brill

- Brill calls on industry to develop best practices "right now" to address the most urgent consumer protection issues raised by IoT

- Best practices would fill gap resulting from lack of federal legislation that would set baseline privacy and security rules for all companies that collect personal data (which FTC has advocated for without success).

Adapting Privacy Best Practices to Connected Devices

- Privacy regulation is based on traditional notions of “notice” and “consent”
  - But those concepts must be adapted to apply to IoT
- Wearable fitness trackers typically don’t have a user interface to serve as a means to present consumers with a choice about data collection
- Connected devices may become too numerous for consumers to effectively manage their information
- Brill urges companies to “get creative” about providing privacy transparency and control for consumers to manage their data
  - Example: “Command center” that runs multiple household devices and can describe in simple terms how information is being collected and used

The FTC Weighs In

- In January 2015, the FTC issued the report “Internet of Things: Privacy & Security in a Connected World”
  - Based on input from technologists, academics, industry representatives, consumer advocates at November 2013 FTC workshop in D.C.
  - Report is limited to IoT devices that are sold to or used by consumers
  - Recommended practices document, does not have the force of law or regulations
  - But may provide insight into future FTC enforcement actions

FTC's IoT Recommendations

- Build security into devices at the outset, rather than as an afterthought in the design process
  - "Security by Design"
- Train employees about the importance of security
- Ensure that security is managed at an appropriate level in the organization
- Ensure that when outside providers are hired, those providers are capable of maintaining reasonable security, and provide reasonable oversight of the providers

FTC's IoT Recommendations (cont.)

- When a security risk is identified, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk

- Consider measures to keep unauthorized users from accessing a consumer's device, data or personal information stored on the network

- Monitor connected devices throughout their expected life cycle and, where feasible, provide security patches to cover known risks

Data Minimization

- The FTC recommends that IoT companies consider data minimization
  - Limiting the collection of consumer data
  - Retaining the information only for a set period of time, not indefinitely

- Data minimization addresses two key IoT privacy risks:

(1) That a company with a vast database of consumer data will become an attractive target for data thieves or hackers

(2) That consumer data will be used in ways contrary to consumers' expectations

Flexible Approach to Data Minimization

- FTC takes a flexible approach to data minimization. Companies can
  - Collect no data
  - Limit data to the categories required to provide the service offered by the device
  - Collect less sensitive data
  - De-identify the data collected

- HIPAA's "minimum necessary" use and disclosure rule provides a useful comparison

Notice and Transparency

- The FTC also recommends that IoT companies notify consumers and give them choices about how their information will be used
  - Particularly when the data collection is beyond consumers' reasonable expectations
  - No one-size-fits-all approach regarding notice
  - Some IoT devices don't even have a consumer interface

- In a 2012 privacy report, the FTC stated that companies shouldn't ***always*** be compelled to provide choice before collecting and using consumer data
  - IF the practices are consistent with the context of a transaction or the company's relationship with the consumer

Choice and the Oven Manufacturer

- Consumer buys a smart oven from ABC Vending
  - Connected to an app that allows the consumer to remotely turn on the oven to the setting “Bake at 400 degrees for one hour”
  - IF ABC uses the consumer’s oven-usage data to improve the sensitivity of its temperature sensor or recommend another ABC product to the consumer
    - No need to offer consumer choice – this is consistent with ABC’s relationship with the consumer
  - IF ABC shares consumer’s data with a data broker or an ad network
    - Use is inconsistent with the context of the consumer’s relationship to the manufacturer
    - Company should provide consumer with choice

Permission Re-delegation

- February 2013: The FTC settles charges with mobile device manufacturer HTC America that it failed to take reasonable steps to secure the software it developed for smartphones and tablet computers

- The FTC cites “permission re-delegation” issues
  - User consents to App A’s use of geolocation data, but App A then shares with App B without user permission

- Settlement included comprehensive security program, conducting independent audits and reporting to the FTC for 20 years, and developing required security patches

Providing Choice Without a Consumer Interface

- The FTC cited some creative options for IoT companies seeking to provide privacy choice without a consumer interface

  – Choices at point of sale: One auto industry workshop participant said they provide opt-in choices at the time of purchase "in plain language and multiple choices of levels"

  – Tutorials: Facebook offers a video tutorial to guide consumers through its privacy settings page. IoT device manufacturers can provide similar tools for explaining privacy choices

Providing Choice Without a Consumer Interface (cont.)

- Codes on the device
  - Manufacturers could affix a QR code or similar barcode that, when scanned, would take the consumer to a website with information about applicable data practices
    - Consumers could then make privacy choices through the website interface
- Choices during set-up
  - Many IoT devices have an initial set-up wizard
  - Can be used to provide clear, prominent and contextual privacy choices
- Management portals and dashboards

Providing Choice Without a Consumer Interface (cont.)

- "Out of band" communications requested by consumers
  - Some home appliances allow users to configure their devices so that they receive important information through emails or texts

- A User Experience Approach
  - Learning from consumer behavior on IoT devices in order to personalize privacy choices
  - Example: a manufacturer that offers two devices could use consumer's preference on one device ("no sharing with third parties") to set a default preference on another
  - Example: A home appliance "hub" that stores data locally could learn a consumer's preference based on prior behavior and predict future privacy preferences as new appliances are added to the hub

Security in the IoT

- In January 2015, the FTC also issued a publication for businesses with advice on how to build security into products connected to the IoT:
  - "Careful Connections: Building Security in the Internet of Things"

- Data security takes on a whole new dimension in IoT
  - An insecure connection could give a hacker access to not just the device, but everything else on a user's network
  - If a home automation system isn't secure, a criminal could override settings and unlock doors
  - A hacker could remotely recalibrate a medical device such as in insulin pump or a heart monitor (the *Homeland*/Dick Cheney scenario)

Is Your Car Hackable?

- February 2015: Sen. Ed Markey supervised a report stating that vehicles are vulnerable to hacking through wireless networks, smartphones, infotainment systems like OnStar – even a malicious CD popped into a car stereo

- January 2015: BMW AG reports that it fixed a security flaw that could have allowed up to 2.2 million vehicles to have their doors opened remotely by hackers

- New risks will arise when vehicles communicate with one another through “vehicle to vehicle” technology to prevent crashes

Risk-Based Approach to Security

- The FTC's "Careful Connections" document recommends a risk-based approach to IoT security
  - Consistent with best practices and other security regulatory regimes

- Inventory the kinds of information you're collecting, which serves to
  - Establish a baseline as staff and product line evolve over time
  - Assist in regulatory compliance
  - Aid in allocating resources to where they're needed most

- FTC cites National Institute of Standards and Technology (NIST) standards for risk assessment

Authentication

- The FTC stresses the importance of strong authentication
  - An authentication failure could lead to unauthorized access to personal information or the consumer's home network
  - If the risks are substantial (based on the volume or sensitivity of the information maintained) consider two-factor authentication
    - Use of a password and a secure token

Protect Your Interfaces

- A security weakness at the point where a service communicates with your device could give scammers a foothold into your network
  - Example: interface between a mobile device and the cloud

- Two interface threats:
  - Cross-site scripting (XSS) attacks: malicious scripts are injected into otherwise trusted websites
  - Cross-site request forgery (CSRF) attacks: unauthorized commands are sent from a user the website trusts

FTC's TRENDnet Enforcement Action

- September 2013: FTC settles its first enforcement action against an IoT product
  - *In the matter of TRENDnet, Inc.*, FTC File No. 122 3090

- TRENDnet sells internet protocol cameras that consumers can use to monitor homes or businesses by accessing live video and audio feeds through a web browser or mobile app
  - Hackers posted live video feeds from about 700 homes after compromising wireless home security cameras

- TRENDnet represented the cameras were secure by
  - Using the trade name "SecurView"
  - Making statements about security in packaging and ads, and on website
  - Providing users the option to require login credentials to access live feeds

FTC's TRENDnet Enforcement Action (cont.)

- FTC charged that TRENDnet failed to provide reasonable security for the cameras
- Live feeds from many camera models were accessible over the Internet to anyone
  - Without login credentials – even if camera user chose that setting
- FTC cites several practices in its complaint that contributed to the security failure
  - Transmitting login credentials via unencrypted text over the Internet
  - Storing login credentials as unencrypted text on users' mobile devices
  - Failing to actively monitor security vulnerability reports from third parties
  - Failing to design and test camera software in a way that provides reasonable and appropriate security

FTC's Unfairness Doctrine

- FTC's jurisdiction in TRENDnet was based in part on the so-called "unfairness doctrine"

- In 2005, the FTC articulated the "unfairness doctrine" in the settlement of an enforcement action involving BJ's Wholesale Club

- Previously, the FTC had based its data security enforcement efforts on its authority to regulate "deceptive," rather than "unfair", acts or practices
  - If a company said nothing about its information security practices, then the FTC had no jurisdiction

FTC's Unfairness Doctrine (cont.)

- The FTC only needs to show that a company's information security practices:
  - Cause or are likely to cause substantial injury to consumers
  - That the harm to consumers is not reasonably avoidable by consumers themselves
  - That the harm is not outweighed by countervailing benefits to consumers or to competition
- Recent LabMD ruling indicates that FTC charges under the unfairness doctrine can be defeated

TRENDnet Consent Order

- TRENDnet consent order with FTC
  - Prohibits TRENDnet from misrepresenting the security and privacy of its cameras
  - Requires TRENDnet to establish a comprehensive information security program
  - Requires TRENDnet to obtain annual third-party assessments of its security program for 20 years
  - Requires TRENDnet to notify customers about security issues with the cameras and a software update to correct them
  - Requires TRENDnet to provide free technical support for updating or uninstalling cameras for two years

Other Regulation of IoT Privacy and Security Issues

- U.S. Dept. of Energy has led multiparty discussion on smart-grid privacy and security issues
- U.S. Dept. of Transportation's National Highway Safety Administration has launched cybersecurity research for motor vehicles
- U.S. Food and Drug Administration has published guidance regarding cybersecurity of networked medical devices
- Federal Communications Commission enforces rules concerning the confidentiality of customer use information collected by wireless network carriers

The Future of IoT Litigation

- March 2015: An early IoT case was filed in U.S. District Court for the Northern District of California against General Motors, Ford and Toyota
  - *Cahen v. Toyota Motor Corporation*
  - Suit claims defendants sold millions of cars that are vulnerable to hacking and their value is diminished because a hacker could take control of steering, braking and acceleration remotely during driving

- IoT lawsuits are likely to gradually gather momentum
  - Limited by the fact that currently most IoT breaches do not lead to severe damages
  - Exception: A German steel mill caught fire and was seriously damaged in 2014 after its business network was hacked to gain access to systems controlling plant equipment
  - Stuxnet computer virus

Hello Barbie Lawsuit

- December 7, 2015: Toymaker Mattel has a proposed class action filed against it in Los Angeles County Superior Court
- Claims that its new interactive doll Hello Barbie violates the Children's Online Privacy Protection Act (COPPA) by recording their conversations with the doll without proper consent
- Plaintiff bought toy for her daughter, registered it online and downloaded smartphone app that would allow parent to listen to, review and delete recordings transmitted to servers of ToyTalk, Inc.
- Daughter and friends had Barbie-themed party where voices of other children were recorded by the toy without parental consent
- Suit alleges negligence, unjust enrichment, invasion of privacy and violations of California's Unfair Competition Law

Establishing Damages

- IoT litigation may also be limited by the nature of the data involved

- Successful security breach litigation has focused on cases where actual financial fraud or identity theft has been committed
  - Credit card numbers and Social Security numbers have a quantifiable value on the black market
  - It is less clear how IoT data, such as the time when a person leaves for work, can be monetized

- However, IoT data is of value to data aggregators, who can use it to develop a consumer profile that can be sold to marketers

The Legal Ramifications of IoT

- The IoT is going to eventually raise a host of complex legal issues around causation, liability and discovery
- Your voice-controlled television records conversations among family members in your home. Is that data subject to discovery?
- Can insurers require access to television voice recordings if it might help assess a claim?
- When a malfunction occurs involving interconnected devices (home thermostat, security system and kitchen) resulting in damages (house fire), how will liability be allocated among the various device manufacturers?
- How will the comparative negligence of the homeowner be determined?

Caremark Derivative Claims

- In the wake of an IoT data breach, it is likely that companies will see more so-called *Caremark* derivative claims
  - Under Delaware law, a *Caremark* claim charges a lack of board oversight of compliance functions, based on violation of the duties of loyalty and good faith
  - Significant because, while the business judgment rule may shield directors from monetary damages for breaches of the duty of care, it does not protect them from breaches of the duties of loyalty and good faith
  - Premised on the seminal case *In re Caremark International Inc. Derivative Litigation,* 698 A.2d 959 (Delaware Chancery, 1996)

Caremark Derivative Claims (cont.)

- In a *Caremark* derivative claim, a plaintiff must show that the defendants either:
  - "Utterly failed" to implement a reporting system or controls OR
  - Consciously failed to monitor or oversee the operations of a reporting system or controls
- In the cybersecurity context, shareholders may assert that management and the board failed to adequately supervise and allocate resources to the company's cybersecurity risk management
  - Ignoring red flags that could have prevented a breach
  - Failing to respond to a breach in a timely, appropriate manner that could have prevented future harm
- Derivative suits are in some ways easier to bring than consumer class actions – a single shareholder can bring one based on an alleged harm to the company

Process Over Perfection

- A post-breach *Caremark* derivative lawsuit filed against hotel chain Wyndham was dismissed in 2014, and it provides valuable guidance for boards
  - The district court's dismissal noted with approval the measures used by the defendants to address the data breaches, including
    - The board discussed the breaches at 14 meetings over a nearly 4-year period, including presentations from the general counsel
    - The audit committee discussed the cyber risk issues at 16 meetings over the same period
    - The company retained a computer forensic firm to investigate the breach and acted upon its recommendations for enhanced cybersecurity
  - The lesson – emphasize Process over Perfection

The Risk to IoT Startups

- The proliferation of new IoT devices has brought many startups to this space
- Often these startups do not take a rigorous approach to privacy and security compliance programs
- Could lead to exposure to *Caremark* claims

Components of a Cybersecurity Compliance Program

- Assessment of company data flows, focusing on areas where there are risks to data
- Written privacy and security policies and procedures (including incident response plan), accompanied by auditing to ensure effectiveness
- Training management and staff on the incident response plan and privacy and security policies and procedures
- Appoint a chief information security officer (CISO) or equivalent position that reports to the CEO or the appropriate board committee
- Regularly retain a security consulting firm to review and test the company's cyber defenses
- The board's cyber committee should be updated quarterly or more frequently on changes to the security program and related findings, with updates to the full board at least annually

NIST Cybersecurity Framework

- On Feb. 12, 2014, the Obama administration released the final version of a much-anticipated voluntary cybersecurity framework
  - Developed by the National Institute of Standards and Technology (NIST) in collaboration with stakeholders
  - At the direction of Pres. Obama's executive order one year prior
  - Focuses on protection of "critical infrastructure"
  - A good starting point for most companies, including IoT companies, seeking to implement reasonable cybersecurity measures

The NIST Framework

- The framework borrows from existing industry security standards and encourages organizations in the critical infrastructure sector to
  - Map out a “current profile” of cyberattack readiness
  - Pinpoint a “target profile” that reflects readiness based on an analysis of the likelihood and impact of a cybersecurity event
  - Identify “gaps” between the profiles
  - Implement an action plan to address those gaps

No Broad IoT Legislation on the Horizon

- FTC states that IoT-specific legislation would be premature at this point given the rapidly evolving nature of the technology
- FTC still calls for federal data security and breach notification legislation
- FTC also calls for broad-based privacy legislation that is flexible and technology-neutral
- Both types of legislation are unlikely to gain traction at this time

As Usual, California Is a First-Mover

- January 1, 2014: California law takes effect restricting disclosure of information about customer electrical or gas usage from the smart grid
  - Cal. Civil Code §§ 1798.98-.99

- Requires businesses with access to this data to maintain "reasonable security procedures and practices"

- Appears to be the first state law specifically addressing an IoT privacy/security concern

ASIA

Almaty
Astana
Beijing
Singapore
Tokyo

EUROPE

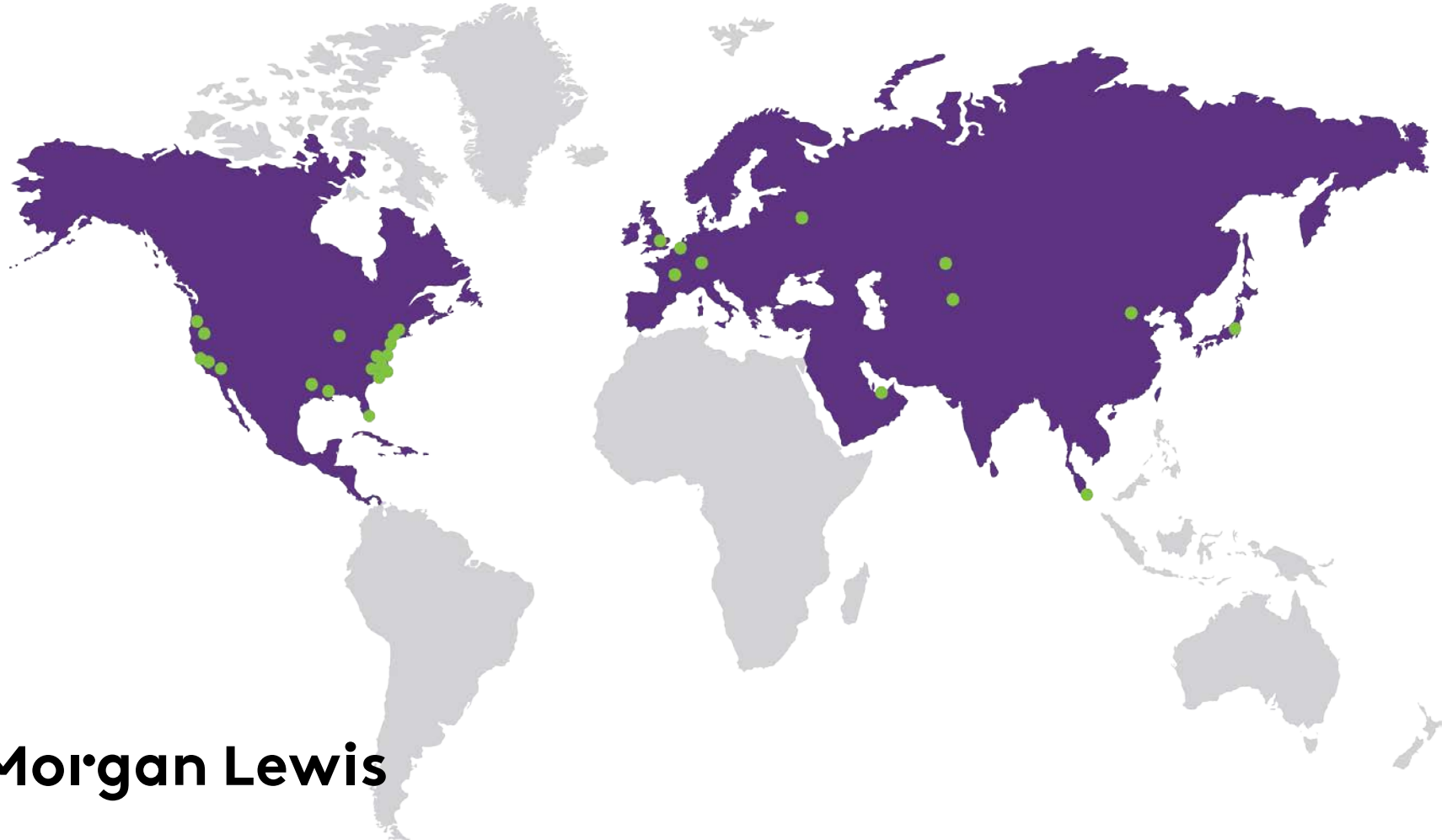
Brussels
Frankfurt
London
Moscow
Paris

MIDDLE EAST

Dubai

NORTH AMERICA

Boston
Chicago
Dallas
Hartford
Houston
Los Angeles
Miami
New York
Orange County
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Washington, DC
Wilmington



Morgan Lewis

Questions?

W. Reece Hirsch
rhirsch@morganlewis.com
(415) 442-1422

Morgan Lewis