MoFo Webinar.

Data Protection Masterclass: Big Data and the Internet of Things - From Theory to Practice

Table of Contents

Presentation ....................................................................................... 1

Speaker Biographies ......................................................................... 2

About Morrison & Foerster ............................................................... 3

Selected Articles and Alerts .......................................................... 4

- Hot Topic: Wearables (E-Commerce Law & Policy article) – June 2014
- The Internet of Things – Part 2: The Old Problem Squared - 20 March 2014
- The Internet of Things – Part 1: Brave New World - 18 March 2014
Presentation

Data Protection Masterclass:

Big Data and the Internet of Things – From Theory to Practice
Data Protection Masterclass:
Big Data and the Internet of Things —
From Theory to Practice

10 June 2014

Karin Retzer
D. Reed Freeman
Stephanie Sharron
Alistair Maughan
Overview

• Where we are with Big Data and what does it mean for your business?
• Prospects for IoT and the likely legal and regulatory factors that will affect the development and growth of IoT technology and the markets that such technology will create
• Privacy and security risks posed by Big Data and IoT, and how regulators in the U.S. and Europe are reacting
• Commercial issues raised by Big Data and IoT, e.g., in terms of (i) cloud computing & outsourcing, (ii) ownership of data and (iii) consumer protection
• Good practice tips on how to mitigate legal risks raised by Big Data and IoT
What is Big Data and the Internet of Things?

Stephanie Sharron
SSharron@mofo.com
Palo Alto

Alistair Maughan
AMaughan@mofo.com
London
What is the “Internet of Things”? 
• The ability for everyday devices to connect with each other and with people
• Today, there are 6 billion devices connected to the Internet
  ➢ By 2020, estimates put that number as high as 50 billion
  ➢ That’s 4-7 connected devices per person
• At present, most smart products are fragmented and do not work together. Data are siloed in each product’s separate app. That will change in the future as devices grow more inter-connected
The term IoT was first coined by the Auto-ID center [AUTO-ID] in 1999, as part of efforts under way with respect to standardizing approaches to RFID tags.

IPv6 and web services simplify deployment by enabling simplified integration with Internet hosts, simplified development of diverse “things” and a unified interface for software.

Different “things” like sensors, RFID tags or appliances can interact with each other, back-end systems and humans that have mobile devices like a tablet or smart phone.
What is a “Thing”

• One way to think about “things” is by their communication patterns (IETF Security Considerations Draft (2013)):
  - human-to-human (H2H)
  - human-to-thing (H2T)
  - thing-to-thing (T2T)
  - thing-to-things (T2Ts)

• Sensors, microcontrollers, sensor hubs, mobile devices and more hubs take in and compute data to relieve processing required on the sensor’s application processor or the microcontroller

• Passive sensors collect and distribute information without the need for a person to activate the sensor each time data are processed
  - Examples: Proteus ingestible pill sensor, Eldercare in-home sensors, Find My iPhone
  - Challenges: more talk about “ransomware”—the ability to threaten someone with physical or other harm—as well as more conventional concerns about unauthorized disclosure and use of data
2014: A Day in the Life…

- Eating breakfast: smart fridge
- Getting dressed: wearable tech
- In the car: connected apps
- The connected workplace
- Shopping and errands
- Personalized retail
- Smart home: from smart thermostats to smart sensors
- Entertainment
Fun!

Magic Band
Big Data

• The ability to analyze large, complex and rapidly changing datasets comprised of structured, semi-structured or unstructured data to gain valuable insights
  - Clustering (structure/commonalities across data)
  - Associations (relationships between actions/items)
  - Classification of data
  - Regression (relationships between input and output data from a process)

Visualization by IBM of user activity on Wikipedia
Big Data and the Internet of Things: A Symbiotic Relationship

Why the internet of things is big data’s latest killer app — if you do it right

by Derrick Harris

**Unintended Consequences: Sensors & the Rise of Ransomware**

Posted on May 27, 2014 by Lisa Suennen

Big Data's Potential in Helping to Secure the Internet of Things

A Massive Market Opportunity Awaits In Analyzing The Internet Of Things
"The major hurdle ... in the [data] analysis layer is the volume of data that edge nodes emit, and the speed with which it must be processed...." Hammond, Forrester Research

As "intelligence" is applied to these data, products and technologies that anticipate our everyday needs and desires emerge—sometimes referred to as "ambient IQ"
Key Functions Required by IoT and Big Data

• Device and Infrastructure Management Platform
  ➢ IoT requires operators to operate software on devices remotely, without taking the network of sensors out of service
  ➢ Security crucial, particularly where remote access to sensors is required

• New Platform-as-a-Service (PAAS) offerings emerging for Big Data
  ➢ Data storage (e.g., supported versions of Hadoop)
  ➢ Data warehousing and database tools
  ➢ Data analytics tools and applications: real-time and predictive

• Data Filtering
  ➢ Vast amounts of data can be generated by sensors
  ➢ Need to filter data to that which is necessary so that systems aren’t overwhelmed

• Analytics Platform
  ➢ Diversity of devices producing data from different locations needs to be configured so that the data can be leveraged
  ➢ Integration with the big data analytics platforms
EU Privacy Issues

Karin Retzer
KRetzer@mofo.com
Brussels
European Framework

- General principles of Data Protection Directive 95/46/EC apply

- Anonymous data are not covered but anonymization requires full de-identification and is difficult
  - Article 29 Working Party (WP29) Opinion 05/2014 on Anonymization Techniques

- WP29 Opinion 3/2013 on Purpose Limitation analyzes the use of big data

- European Commission public consultation on IoT
  - Policy document to be issued as part of EU Digital Agenda
Basic Principles

• Legal Basis
  ➢ Personal data may be collected if there is a “legitimate interest” or with explicit consent

• Purpose limitation
  ➢ Personal data must be collected for “specific, explicit and legitimate purposes” (*purpose specification*) and
  ➢ Not be “further processed in a way incompatible with those purposes” (*compatible use*)
  ➢ Subject to specific safeguards, further processing for historical, statistical or scientific purposes is not incompatible

• Data minimization
  ➢ Personal data must be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”
Basic Principles (Cont’d)

• Data retention
  ➢ Personal data must be kept *no longer than necessary* to achieve the purposes for which the data were collected

• Automated processing
  ➢ Individuals have the right to not be subject to decisions based solely on automated processing

• Access rights
  ➢ Individuals have the right to know what data is held about them and rectify or delete the data

• Data transfers
  ➢ Data held outside the EU/EEA or stored in the EU/EEA but accessed from outside is subject to transfer limitations
WP29 Opinion on Purpose Limitation

• WP29 acknowledges the benefits associated with the use of big data for research and innovation

• WP29 stresses that big data entails certain privacy risks:
  - Tracking and profiling based on a combination of data from different sources
  - Limited transparency
  - Inaccurate analytics results
  - Highly intrusive personalized advertising
  - Poor data security
  - Increased risk of government surveillance
Purpose Specification

- Purpose for data processing must be:
  - **Specific** – precisely and fully identified before or (at the latest) during data collection; organizations should be able to predict the data uses
  - **Explicit** – clearly communicated in an intelligible and transparent form (i.e., to ensure that individuals have the same understanding irrespective of cultural or linguistic diversity)
  - **Legitimate** – legally justified (also based on other areas of law); in addition, there must still be legal grounds for processing (consent, balance of interest or legal necessity)

- Further processing for a different purpose
  - All new or different purposes must be specified
  - All other criteria (specific, explicit and legitimate) must be satisfied
Secondary Use

- Directive prohibits incompatibility rather than requires compatibility

- Processing which is incompatible with the purposes specified at collection is unlawful and therefore prohibited
  - Organization must not use a new legal basis (consent, legitimate interest or legal necessity) to justify a new processing activity disconnected from the previous one
  - A simple change of privacy policy is not sufficient to legitimize a new, incompatible purpose

- Compatibility must be assessed on a case-by-case basis
  - A new purpose is not automatically incompatible
  - Use of data for historical, statistical or scientific purposes is generally compatible, provided adequate safeguards are in place (data minimization, anonymization, privacy-enhancing techniques, etc.)
Compatibility Test

• Organizations should conduct a “compatibility test” that takes into account the following:
  ➢ The relationship between the purposes for which the personal data have been collected and the purposes for further processing
  ➢ The context in which the personal data have been collected and the reasonable expectations of the individuals regarding further use
  ➢ The nature of the personal data and the impact of further processing on the individuals
  ➢ The safeguards adopted by the organization to ensure fair processing and to prevent any undue impact on the individuals

• WP29 calls for a “rigorous but balanced and flexible application” of the compatibility test
IoT – Privacy Issues

• Which law applies?
  ➢ Devices and data centers are located in many countries
  ➢ EU/EEA law applies to any non-EU/EEA organization using equipment located in the EU/EEA to process data

• What individuals are covered?
  ➢ Individual customers, patients, employees, children, etc.

• When are data collected and by whom?
  ➢ Devices are able to communicate with each other and transfer data autonomously without individuals being aware of it
  ➢ Risk of permanent surveillance
  ➢ Scope of individual’s control – privacy button
IoT – Privacy Issues (Cont’d)

• Organizations must demonstrate legitimate interest or obtain consent
  ➢ Consent is often not an option, e.g., when data is collected via the device from employees

• Data security – multilayered and expensive to implement
  ➢ Physical security – devices must be secured with locks, alarms, etc. to prevent data loss when they are stolen or lost
  ➢ Network security – communication should be encrypted or secured in another way
  ➢ Data security – data stored at the device should be encrypted to prevent compromise of information

• Risk of data use for incompatible purposes
Big Data: Scenario 1 – Targeting Users

- Big data is used for personalized discounts, special offers and targeted advertising
- Specific, free, informed and unambiguous **opt-in consent** is almost always required, including for:
  - Tracking and profiling, direct marketing, behavioral advertising, data brokering, location-based advertising or tracking based on digital market research, etc.
- Organizations should:
  - Provide easy access to profiles
  - Disclose their underlying decision criteria (algorithm)
    - Potential CONFLICTS with trade secrets protection
    - According to WP29 it must not limit the disclosure under data protection rules
  - Disclose source of the data that led to the creation of the profile
  - Allow data portability
- Individuals should be able to correct or update their profiles and have direct access to their data in a portable and user-friendly manner
Big Data: Scenario 2 – Predicting Trends

• Big data is analyzed for predicting trends – no major issues
• Need for functional separation
  ➢ Data used for statistical or other research purposes should not be used for other purposes directly related to individuals (unless specifically authorized by the individuals)
• Emphasis on security
  ➢ Data controllers must guarantee data confidentiality and security and take all necessary technical and organizational measures (e.g., anonymization, pseudonymization and aggregation)
IoT: Scenario 3 – Telematics

- Data is collected via devices installed in vehicles for monitoring movement
- Need to demonstrate legitimate interest
  - For example, that data is necessary to optimize fleet management, optimize personnel management, prevent risks of accidents, prevent other damage or loss of life, calculate insurance premiums, improve driving techniques, etc.
  - Consent problematic
- Some purposes may need to be reached by less privacy intrusive means; the following should be avoided:
  - Continuous employee compliance monitoring
  - Monitoring employees’ respect of speed limits
  - Monitoring employees working on flexible hours schedules
  - Monitoring employees outside working hours when the vehicle is used for private purposes
  - Facial recognition technology unless purposes cannot be achieved otherwise
IoT: Scenario 3 – Telematics (Cont’d)

- Emphasis on appropriate notice
  - Organizations should have in place appropriate internal privacy policies and procedures explaining what data are collected, why and how data can be accessed
  - Additional sticker notice in a vehicle is recommended
- Technical means of disabling data collection
  - Privacy button
- Access, correction, objection and deletion rights must be provided
- Arrangements with data recipients and processors must be put in place
- Data must not be used for any other purpose
Practice Tips

• Identify and manage responsibilities
  ➢ Identify your responsibility in collecting and using of data and related privacy obligations
  ➢ Ensure contractual arrangements with players involved in data cycle

• Ensure legal basis
  ➢ Demonstrate that data collection is necessary to achieve purposes and that the least privacy-intrusive methods were employed
  ➢ Avoid relying on consent where consent may be withdrawn or is questionable (employment)

• Be specific
  ➢ Avoid informing about purposes that are too vague or too general
    ▪ For example, improving user experience, marketing purposes, IT security purposes and future research
  ➢ Provide granular information to ensure all of the different purposes are sufficiently clear
    ▪ For example, an organization providing various services (email, social networking video and music uploads) should provide specific details
Practice Tips (Cont’d)

- Include more details where purposes cannot be clearly derived from the context
- Use layered notices
  - Key information should be presented in a concise and user-friendly manner (e.g., by displaying an icon) while more detailed information should be accessible via links
- Break down general purposes
  - For example, instead of saying “processing an individual’s claim for a social benefit,” the notice should say “verifying the individual’s identity, carrying out various eligibility checks, checking other benefit agencies’ records, etc.”
  - General purposes are, however, useful when providing layered notices
Practice Tips (Cont’d)

- Apply other general data protection rules
  - Retain data no longer than allowed or required
  - Ensure appropriate security
  - Ensure exercise of access and correction rights
  - Restrict access and implement access controls
  - Address transfer restrictions
  - Register database and obtain data protection authority authorizations, where required

TIPS!
Looking Ahead

• Draft Data Protection Regulation
  ➢ Intended to harmonize data protection rules across the EU/EEA
  ➢ Draft was approved by the European Parliament on March 12, 2014
  ➢ To become law, the draft Regulation must still be approved by governments of all 28 EU Member States – timing is unclear

• Draft Regulation will significantly impact big data and will set out requirements for IoT

• EU politicians voice stronger opinions
  ➢ Viviane Reding commenting on the recent ECJ’s Google judgment said “Companies can no longer hide behind their servers being based in California or anywhere else in the world.” … “Big data needs big rights”
Impact on Big Data and IoT

• Applicable law
  ➢ Regulation would apply to any EU/EEA and any non-EU/EEA organization that monitors EU/EEA residents or offers goods or services to them

• Detailed notice requirements
  ➢ Privacy notices and policies must include detailed information and be preceded by privacy icons

• Consent
  ➢ Explicit consent is likely to be the norm
  ➢ Consent may not be used as basis for processing additional data that are not necessary for provision of main service

• Data portability
  ➢ Individuals have the right to obtain copy of all their data in an intelligible electronic format

• Impact Assessment
  ➢ Obligation to conduct data protection impact assessment for any processing relating to 5000 or more individuals or that involves profiling
Impact on Big Data and IoT (Cont’d)

- Privacy by design and by default
  - Devices and applications must be designed to minimize data collection and storage by default and have “data protection-friendly” settings
  - Individuals must be able to control the distribution of their personal data
  - Cost of implementation is no longer a mitigating factor

- Profiling
  - Profiling that has legal effects on individuals or significantly affects their rights and interests permitted only with explicit consent
  - Some flexibility possible for processing pseudonymous data but only if individuals’ identification is impossible
  - “Human assessment” needed for decisions affecting individuals

- Stricter conditions for processing data for historical, statistical or scientific research purposes
  - Processing is permitted if purposes cannot be otherwise achieved and re-identification of the individuals is avoided
• The Article 29 Working Party’s Opinion 03/2013 on Purpose Limitation

• The Article 29 Working Party’s Opinion 05/2014 on Anonymization Techniques

• Draft Data Protection Regulation (as adopted by European Parliament on March 12, 2014)

• European Commission’s report on the consultation on IoT
U.S. Privacy Issues

D. Reed Freeman
RFreeman@mofo.com
Washington, D.C.
General U.S. Regulatory Concerns

• The collection and analysis of “big data” can be used to directly affect individuals, and can be based on personally identifiable information
  ➢ This collection and analysis can happen without consumers knowing or understanding what is going on

• In other words, big data raises privacy concerns:
  ➢ The sheer scale of data collection, tracking and profiling, also taking into account the variety and detail of the data collected and the fact that data are often combined from many different sources
  ➢ The security of data, with levels of protection shown to be lagging behind the expansion in volume
  ➢ The transparency of data; unless individuals are provided with sufficient information, they will be subject to decisions that they do not understand and have no control over
  ➢ The inaccuracy, discrimination, exclusion, stereotyping and de-individualism of data (echoing FCRA issues)
  ➢ The increased possibilities of government surveillance
U.S. Regulatory Outlook - Overview

• Federal Trade Commission on Big Data and the Internet of Things
  ➢ Data Brokers Report (May 2014)
    ➢ Arises out of Data Broker Investigation that began in late 2012, calls for legislation
  ➢ Privacy Report (March 2012) & Big Picture Workshop (December 2012)
  ➢ Commission speeches, including:
    ➢ Chairman Ramirez speech on “Privacy Challenges of Big Data” (August 2013)
    ➢ Commissioner Brill speeches including “Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data” (June 2014)
  ➢ TRENDnet Internet of Things Enforcement Action (December 2013)
    ➢ Big Data Enforcement Actions Coming Next?

• Congress
  ➢ Senate Commerce Committee report and hearing on data brokers

• Obama Administration Big Data Study (May 2014)
FTC 2014 Data Broker Report

- The FTC Data Brokers Report released May 27, 2014
  - Based on investigation of nine data brokers that began in December 2012
    - Data brokers are companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies
- FTC concerns identified in the report are not new:
  - Transparency
  - Sensitivity of data collected, and its potential uses
  - The accuracy of the data, and the ability to correct inaccurate information
  - Security and the risk of identity theft
- In light of the concerns raised in the Data Broker Report, the FTC calls on Congress for legislation to enhance transparency, protect sensitive data and ensure that data is accurate
The Privacy Report was the first foray into Big Data

- Included a call for “targeted legislation” to provide consumers with access to information held about them by data brokers in order to “address the invisibility of, and consumers’ lack of control over, data brokers’ collection and use of consumer information”
- Called on data brokers “to explore creating a centralized website where data brokers could:
  - (1) identify themselves to consumers and describe how they collect and use consumer data and
  - (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.”
- One data broker, Acxiom, had already created such a portal: https://aboutthedata.com/
  - the FTC has now called for Congress to require such portals by law

The Privacy Report also noted that companies that collect information about consumers and combine it with information from data brokers (e.g., “data append”) should take steps to be more transparent about this practice
FTC Workshop: The Big Picture

- December 2012 workshop discussing Comprehensive Online Data Collection (e.g., Big Data)
- Panelists generally agreed:
  - Data collection policies should be technology neutral
  - There are tangible benefits from large-scale online data collection
  - Certain data uses are improper (e.g., redlining)
  - Competition and innovation should be encouraged
- Panelists disagreed about:
  - The scope and nature of harms to consumers from comprehensive data collection
    - Does harm only flow from the misuse of the data, or from the collection itself?
  - Whether consumers actually are aware of this collection
  - Whether regulation is necessary
FTC Commissioners’ Views

• Chairwoman Ramirez, in “The Privacy Challenges of Big Data: A View from the Lifeguard’s Chair,” Keynote Address at Aspen Ideas Forum, August 19, 2013, lays out her view of the risks of big data
  ➢ Indiscriminate collection, making sure consumers have meaningful consumer choice, data breaches, profiling and “data determinism”
    o “Data determinism” is the concern that big data will be used “to make determinations about individuals, not based on concrete facts, but on inferences or correlations that may be unwarranted

• Commissioner Brill is concerned about more than just use, as indicated by her June 2, 2014 speech on “Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data”
  ➢ “Use- and risk-based regulatory approaches are important, even necessary, but they are not sufficient. They don’t cover all the droplets of small data—much of it from interactions consumers have with their favorite online retailers, social media sites, and apps—that flow in surprising ways, out of context of the original interaction, into the rivers of big data”
    o “Today, the quantity of personal information sucked into the cyber-vortex is growing exponentially”
    o “The Internet of Things will exponentially expand the deeply personal information that is the data broker’s fodder”
FTC and the Internet of Things

- FTC held a workshop examining privacy and security issues surrounding the internet of things in November 2013. Key themes:
  - Risks to consumer privacy from the collection, analysis and unexpected uses of large amounts of data about consumers
  - Possibility that traditional notice and consent frameworks will not be sufficient to inform consumers of how their personal data is being used
  - Data security risks of interconnected objects

- *In re TRENDnet* (December 2013)
  - First-ever “Internet of Things” case against the maker of a surveillance camera system with a range of uses from home security to baby monitoring
  - Cameras had a faulty software configuration; nearly 700 live camera feeds accessed by a hacker
    - FTC alleged that the company’s failure to reasonably secure its cameras against unauthorized access violated Section 5

- Commissioner Brill has tied the Internet of Things to Big Data
  - In a February 2014 speech, she expressed concern that data from devices—that consumers might not even know are actually connected to the Internet—can be combined with existing troves of data to make it even easier to make sensitive predictions about consumers, such as those involving their sexual orientation, health conditions, religion and race
Commerce Committee Report

- "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes" (December 2013)
  - "Since consumers generally do not directly interact with data brokers, they have no means of knowing the extent and nature of information that data brokers collect about them and share with others for their own financial gain"

- Report focuses on “the collection and sale of consumer data specifically for marketing purposes,” because there is currently very little statutory consumer protection for these uses
  - Expresses concern about segmentation, especially based on financial characteristics, because it can “end up in the hands of predatory businesses seeking to identify vulnerable consumers” or be used to engage in differential pricing
Administration Big Data Report

- **Big Data: Seizing Opportunities, Preserving Values** includes 6 policy recommendations:
  - Department of Commerce should advance a Consumer Privacy Bill of Rights and draft legislative text for consideration by Congress
  - Congress should pass a data breach notification law
  - The Privacy Act of 1974 should apply to non-U.S. persons to the extent possible
  - Privacy regulations must protect against inappropriate sharing or use of information collected on students for education purposes
  - Improve the technical expertise of civil rights and consumer protection agencies to combat big data practices that have a discriminatory impact
  - Amend ECPA to raise the level of online protection to match that provided in older technologies
- Note the divergence between White House and Commissioner Brill
  - Big Data Report says “What really matters about big data is what it does. . . .”
    - Focuses is on harms from use of big data
  - Commissioner Brill says we must give consumers notice and choice regarding *collection*—the “droplets of small data” that “flow in surprising ways, out of context of the original interaction, into the rivers of big data”
    - Use-based approaches are “not sufficient”
- Department of Commerce has now requested comment on whether White House Privacy Bill of Rights should be amended to focus on uses of data
Looking Ahead

• So far, the legislative focus and regulatory response to Big Data—and the rhetoric about it—has focused on data brokers
  ➢ But many, many businesses, from social media networks to major retailers, also collect and analyze large amounts of consumer data
• There are FTC investigations relating to the collection, use and sharing of data that come under the umbrella term “big data.”
• Workshop on Sept. 15, 2014, entitled “Big Data: A Tool for Inclusion or Exclusion?”
  ➢ Will examine both the positive and negative effects of big data, especially on low income and underserved populations
Practice Tips

• At the “Big Picture” Workshop, Commissioner Brill noted that big data collection and comprehensive tracking can lead to “databases of ruin.”
  ➢ Make it difficult to disguise information about ourselves
  ➢ Can harm employment, financial opportunities, reputations
  ➢ Noted that harm that may flow from such databases “falls more directly in the FTC’s wheelhouse”

• Practice Tip
  ➢ Though Commissioner Brill was talking about the companies collecting the data, it is a small step from looking at the practices of those who collect to the practices of those who use.
    o May require heightened notice—consumers may not understand the scope of data used!
  ➢ When using big data for append or other purposes, consider whether a reasonable consumer would understand. That will likely be the Notice & Choice trigger.
Practice Tips (Cont’d)

• Know who is sharing with you
  ➢ Ensure that the data that they share with you are data they have the right to collect
    o E.g., have they provided appropriate Notice and Consent?
    o Frostwire: Deceptive default settings allow broader sharing for consumer data than consumers expect
    o HTC America: Device manufacturer’s security procedures allow certain programs shipped with the phone, as well as malware, to bypass consumer privacy protections

• Know who you are sharing with
  ➢ Ensure that they agree to provide accurate and appropriate notice and choice in a conspicuous place
  ➢ Check periodically to ensure that they are living up to their bargain
  ➢ Ensure that they are using data only as they have represented that they will
Commercial Issues

Stephanie Sharron
SSharron@mofo.com
Palo Alto

Alistair Maughan
AMAughan@mofo.com
London
The Lifecycle of a “Thing”
# Lifecycle of “Thing”: Commercial Agreements

<table>
<thead>
<tr>
<th>Lifecycle Stage</th>
<th>Type of Agreement</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design and Development</td>
<td>Professional Services Agreement</td>
<td>Privacy by Design</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Contract Manufacturing Agreement</td>
<td>Security</td>
</tr>
<tr>
<td>Installation</td>
<td>Services Agreement with third-party installers</td>
<td>Security; Establishing privacy defaults and settings</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>Hand-off back to Manufacturer</td>
<td>Security; Liability; Data Ownership; IPR; Privacy</td>
</tr>
<tr>
<td>Maintenance and Support</td>
<td>Third-Party Services Agreements</td>
<td>Security; Liability</td>
</tr>
<tr>
<td>Decommissioning/Recomm-issioning of Devices</td>
<td>Third-Party Services Agreements End User Agreements</td>
<td>Security; Privacy settings Data transfer; Lock-in</td>
</tr>
</tbody>
</table>
### IPR Issues

Who owns the IPR in the data collected?

<table>
<thead>
<tr>
<th>IPRs</th>
<th>Data Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Copyright</td>
<td>• Proprietary data</td>
</tr>
<tr>
<td>• Database right</td>
<td>• Open data</td>
</tr>
<tr>
<td>• Moral rights</td>
<td>• Creative commons data</td>
</tr>
<tr>
<td>• Trade marks</td>
<td>• Public domain data</td>
</tr>
<tr>
<td>• Trade secrets or confidential information</td>
<td></td>
</tr>
</tbody>
</table>

Big data involves analytics which requires copying and processing the data.

**Key question**: Are your ownership & license rights wide enough to cover the intended use?
Data Ownership/Rights

- Data rights typically derive from data ownership and corresponding rights of use
- Ownership varies depending on the type of data
  - Individual: personal data
  - Corporation/entity: data arising from the activities of a corporation or other entity or persons performing services on its behalf
  - University data
  - Government data
  - Data in the public domain
- But this is oversimplified
  - Consider the wide variety of data that can be used to derive information about an individual or corporation’s behavior; the individual data stream from which the behavioral information derives may belong to many different persons and entities
- Need for a common “data rights framework”?
Supply Chain Issues

- Clearly identify the supply chain
  - Distinguish proprietary platforms and open/SaaS platforms
  - Address integration issues – who takes that risk?
- Define hand-over points
- Service availability and response time service levels
- Scalability – of solution and price
- Define pricing/licensing metrics and counting rules
- Limitations on use?
- Address geolocation issues
- Exit issues
- Alignment of contractual protection?
How are Connected “Things” Different: Liability

• Liability does not arise solely from the object itself (which then can easily be traced back to the owner of the object), but also from the connectedness of the object to other objects, typically through a network of sensors
• Liability “turns on the way that the ‘thing’ interprets, processes and returns the data received” (Barbry, 2012)
• As “things” are deployed and connected in new and novel ways, we will be challenged to allocate who is ultimately responsible for harm and new theories of liability may emerge
• Autonomous communication: “things” are able to communicate autonomously without or with only minimal human intervention
• A requirement to predict the future?
Liability

- Unauthorized access and control of devices can result in a variety of types of harm
- Threats to the Individual
  - Threats to physical safety: planes, trains and automobiles (Personal Injury/Property Damage)
  - Ransomware (Economic and physical harm)
  - The changing face of identity theft: Identity extends to our objects, to the “things” that track our behavior and can then be used to threaten us personally.
  - Other types of criminal activity or wrongful conduct
- Threats to corporations and other entities
  - Corporate theft and espionage
  - IP
  - Tangible property
  - Physical security
  - Data security
- Managing Risk
  - IP reps
  - Legal Compliance programs: consent to use data, privacy policies, data breach notification, etc.
  - Security Procedures
  - Contractual Indemnity: tied to above
  - Insurance
- Traditional allocations may need to be re-examined
- Address holistically across entire range of contractual arrangements
Conclusions & Takeaways

• IoT and Big Data present significant legal challenges
  ➢ Compliance with Law, Global Commerce and Managing within a Changing Legal Landscape
  ➢ Privacy
  ➢ IPR and Data Ownership

• Focus on:
  ➢ Creating the engine
  ➢ Licensing-in the “raw material”
  ➢ Licensing-out the “finished product”

• Understand the data – and track issues accordingly
• Focus on Privacy by Design
• Understand the supply chain and address its issues
• Track the legal and regulatory developments
Thank you!

Karin Retzer
KRetzer@mofo.com
Brussels

D. Reed Freeman
RFreeman@mofo.com
Washington, D.C.

Stephanie Sharron
SSharron@mofo.com
Palo Alto

Alistair Maughan
AMaughan@mofo.com
London
Speaker Biographies

Data Protection Masterclass:
Big Data and the Internet of Things – From Theory to Practice
Alistair Maughan is a partner in Morrison & Foerster’s London office. He is co-chair of the Technology Transactions Group and a member of the Global Sourcing Group.

Mr. Maughan focuses on commercial contracts and technology-based projects for major companies and public sector organisations. His primary areas of expertise include advising on: commercial licensing and sales contracts in the UK and Europe; service-based outsourcing transactions; technology delivery models such as cloud and as-a-service platforms; contracts for the supply and acquisition of technology equipment, services and software; agency and distribution contracts; advising on issues and contracts related to e-commerce; and drafting, negotiating and advising on all types of technology contracts and issues.

His notable transactions include advising Her Majesty’s Revenue & Customs on Europe’s largest "second generation" outsourcing; advising the UK police on its national fingerprint identification system and its project for the delivery and operation of the national UK emergency mobile radio network; advising the world’s largest insurance broker on offshore outsourcing; and other transactions on behalf of government departments, banks, global pharmaceutical companies and major professional services firms.

He has advised on commercial product sales, distribution and supply chain logistics agreements for clients as diverse as UPS (global delivery and logistics company); AIG (global insurer); Novartis (global pharma business); Otto Group (large German retailer); ElectraTherm (innovative U.S.-based provider of heat-from-waste generators); LogiXML (U.S. software company); and Panasonic (major Japanese electronics manufacturer).

For many years, he has counseled both government entities and private sector bidders on procurement law issues and public sector contracts. He has also advised on a number of infrastructure and public/private partnership projects, especially in relation to telecommunications networks and PPP projects in Europe. He edits the firm’s European Procurement and Government Contracts Digest.

Mr. Maughan is a highly regarded commercial lawyer with recommendations in Legal 500, Chambers Global and Chambers UK and Euromoney’s Expert Guides leading independent guides to the legal profession. Chambers UK awarded Mr. Maughan the top ranking for both Outsourcing and Information Technology, commenting that he “brings common sense to the negotiating table.” Other guides note that Mr. Maughan is “the best lawyer ever when it comes to acting for the customer end of the market” and “absolutely excellent when it comes to advising customers on public sector projects.”


Mr. Maughan has a law degree from Leicester University and qualified as a solicitor in 1987. He has practised law on both sides of the Atlantic and is also admitted to the New York Bar.

Follow him on Twitter at @ICToutsourcelaw (http://twitter.com/#!/ICToutsourcelaw).
Stephanie Sharron is partner in the Palo Alto office and a member of the firm’s Technology Transactions Group. Clients turn to Ms. Sharron for advice on the issues that apply to their business models in light of the rapid changes in business, technology and law. She counsels companies in connection with technology and intellectual property transactions and related privacy, data security, and Internet safety issues. Ms. Sharron has represented companies across industries and technologies, including online businesses, cloud services, big data, e-commerce, mobile, life sciences, financial and health IT, digital media, retail, automotive, cleantech and semiconductors, among others.

Ms. Sharron also advises on the commercial technology and intellectual property aspects of mergers, acquisitions, asset spin-off transactions and private equity investments.

Representative matters include:

- Cloud services, software-as-service, platform-as-service, e-commerce, mobile app and other online agreements
- Senior counsel to emerging companies
- Global strategic collaborations for companies across industries, including preparing and responding to RFPs, assisting with evaluation and down-selection processes, and preparing and negotiating definitive agreements
- Manufacturing, distribution and sale arrangements for hardware, semiconductor and other products and services
- Systems integrator and development agreements
- Counseling and re-negotiation of disputed technology-related agreements
- Sourcing and IT procurement
- IP licensing
- Privacy, data security and Internet safety counseling
- Open source counseling
- Intellectual property and technology issues in venture investments, mergers, acquisitions and asset sales

Ms. Sharron is recognized as a 2014 “IP Star” by Managing Intellectual Property, and has been ranked among the top IT & Outsourcing attorneys in the U.S. by Chambers USA in 2012 and 2013. She was also ranked as one of America’s Top Business Lawyers by Chambers USA from 2006-2008.
Reed Freeman is called upon by some of the world’s largest most innovative brands to assist with cutting edge privacy, data security, advertising, and direct marketing issues in the offline, online, mobile, and social media environments.

Mr. Freeman serves as lead counsel in FTC and state consumer protection investigations and negotiations, having handled dozens of such matters since he left the FTC and joined private practice in 1997. He also represents clients in false advertising disputes in federal court before the National Advertising Division of the Council of Better Business Bureaus, Inc., and the National Advertising Review Board. Mr. Freeman is perennially ranked by Chambers and Legal 500 as one of the country’s leading practitioners in the privacy and data security area, and is frequently called upon to speak as a thought leader in the area.

Mr. Freeman also advises a wide variety of clients on deploying, or hiring vendors to deploy, behavioral advertising, retargeting, location-based advertising, personalized content, the use of analytics, and other uses of online, mobile, and social media tracking and targeting technologies. He also counsels clients on compliance with FTC and state advertising laws, in online, mobile, and social media environments. His clients run the gamut from retailers, software companies, hardware manufacturers, to online publishers, advertisers and advertising service providers (including providers of online and mobile analytics), online and mobile application developers (including those that use location-based data), data aggregators, hospitality companies, companies that offer advertising services based on social media, and an email marketing trade association.

Mr. Freeman’s counseling practice includes advising clients on compliance with FTC and state trade regulation issues, including: the Children’s Online Privacy Protection Act, the CAN-SPAM Act, the Telemarketing Sales Rule and its “do not call” rules, the Video Privacy Protection Act and state analogs; California’s Song-Beverly Act, Shine the Light Act, and CalOPPA (including its new Do Not Track elements); state security regulations and data breach notification laws; and self-regulatory principles such as the NAI Code of Conduct, the DAA Self-Regulatory Principles, and self-regulatory principles published by the Council of Better Business Bureaus.

Mr. Freeman is co-author of CCH’s Advertising Law Guide and CCH’s Privacy Law for Marketers. He previously served as staff attorney in the FTC’s Bureau of Consumer Protection and as an adjunct professor of advertising law at George Mason University School of Law. Mr. Freeman received his B.A. from the University of Richmond and his J.D. from the University of Virginia School of Law.
Karin Retzer’s practice focuses on the legal aspects of data protection and security, direct marketing, and electronic commerce.

Ms. Retzer assists clients with privacy and data security compliance and risk management, involving both national and international multi-jurisdictional dimensions. She advises on questions regarding data transfers, the handling of information in shared service centers and sourcing transactions, e-discovery, breach notification, and the use of email and the Internet in the workplace. She has drafted privacy policies and guidelines, notices, agreements for data list management, and data transfer and processing contracts for dozens of multinational clients. She also assists clients in their dealings with data protection authorities, developing appropriate responses to requests for information and complaints, and provides legislative and policy advice to clients. Additionally, Ms. Retzer assists clients with privacy audits and data protection complaints and litigation.

Ms. Retzer has particular expertise regarding the implications of legislative restrictions for online tracking, analytics, personalization of Internet content, behavioral advertising, and direct marketing communications. She regularly advises clients on the use of location data gathered through smart phones and location-based services.

In addition, Ms. Retzer advises clients on issues relating to electronic commerce, such as online terms of use, the requirements for online contracts, disclosure obligations, liability for website content, and the legal aspects of online auction sites. She has developed template agreements and negotiated complex commercial agreements for many clients, counseling them not only with respect to legal ramifications, but also taking into account applicable business and technical considerations. Ms. Retzer is listed as a key individual in The International Who’s Who of Information Technology Lawyers 2013.

Her work spans a wide range of industry sectors. Clients include internationally renowned consumer product companies, financial services organizations, technology and telecommunications providers as well as clients in the advertising, hospitality, media and entertainment, healthcare, pharmaceutical, and retail industries.

Prior to joining Morrison & Foerster, Ms. Retzer worked in Paris at the European headquarters of Sterling Commerce, a U.S. supplier of e-commerce products. From 1997 to 1998, Ms. Retzer worked at the European Commission, where she was involved mainly with examining and monitoring Member States’ implementation of European Community directives.

Ms. Retzer regularly writes for a wide variety of publications. She is a member of the IAPP Publications Advisory Board and a contributing author in the publication, Employee Privacy: Guide to US and International Law. She is a member of the Munich bar and the Brussels EU bar, after studies in Regensburg (Germany), Utrecht (The Netherlands), and Munich (Germany). Ms. Retzer is fluent in German, English, and French and has a working knowledge of Dutch. She is a member of the International Association of Privacy Professionals, the German Association for Data Protection and Data Security, the Licensing Executives Society, and the Association for Industrial Property and Copyright Law.
About Morrison & Foerster

Data Protection Masterclass:
Big Data and the Internet of Things – From Theory to Practice
Firm Overview

Founded in 1883, Morrison & Foerster is now a preeminent global law firm dedicated to delivering business-oriented results to clients around the world. Dynamic technology and life science companies, large financial institutions, leading consumer product companies, and other market leaders come to MoFo for legal knowledge, innovation, and business aptitude. With over 1,000 lawyers spread across 17 offices in the world’s key financial and technology centers, MoFo handles some of the world’s largest cross-border transactions and resolves major disputes across multiple jurisdictions. The firm’s open culture provides every client with access to cross-disciplinary experts across the firm’s offices.

Our attorneys share high standards and a commitment to excellence. Our dedication to serving client needs has resulted in enduring relationships and a record of high achievement. We are a leader in each of our practice areas, including litigation, financial services, intellectual property and technology, tax, and transactional work, such as corporate, M&A/private equity, capital markets, and real estate finance.

Our achievements have not gone unnoticed. *Chambers Global* has named Morrison & Foerster its 2013 USA Law Firm of the Year. *Law360* selected seven MoFo practices as Practice Groups of the Year – more than any other firm. And we have been named to the coveted *American Lawyer* A-List for ten straight years. Of all the Am Law 100 firms on the list with $1 billion or more in revenue, we have the highest combined score in diversity and pro bono. We believe that this demonstrates that MoFo has succeeded financially not despite our cultural values, but because of them.

A MoFo lawyer is something special – a creative and innovative lawyer focused on real-world business results. MoFo lawyers do not dispassionately dispense legal advice. We are in the trenches instead, tirelessly advocating for our clients. It’s where we prefer to be.
MoFo’s International Platform

Over the past three decades, MoFo has developed a world-class international practice – leaving us well-positioned to serve clients across the rapidly expanding global economy. Our international service platform features expertise in M&A, securities, finance and trade, and dispute resolution and includes complex global tax structuring, counsel on foreign workforces, the navigation of regulatory bottlenecks in multiple jurisdictions, and antitrust, environmental, and litigation risk analyses throughout the world.

- We enjoy unrivaled reach around the Pacific Rim with nearly 200 lawyers in Asia teamed with more than 500 lawyers in California.
- We are the largest U.S. law firm in Japan, with more than 120 attorneys in Tokyo, including nearly 50 bengoshi admitted to practice in Japan. With our partners, Ito & Mitomi, we are widely recognized as having Japan’s leading corporate practice.
- Our nearly 30-year presence in China has produced a strong platform of more than 70 multilingual U.S., PRC, and/or Hong Kong-qualified professionals.
- Our newest office in Berlin provides substantial resources to clients in Germany, across Europe, and throughout the world, and has a particular focus on the TMT sector.
- With an established presence in the UK for more than 30 years, we have over 50 lawyers qualified in the UK offering expertise across all major disciplines.
- Through our Brussels office we assist clients that have European Union antitrust and competition issues, including clearance of cross-border mergers and acquisitions, as well as privacy and trans-border data protection matters that affect global companies.
Morrison & Foerster has a world-class privacy and information security practice with more than 60 lawyers from across our global offices actively counseling, litigating cases, and representing clients before regulators around the world on privacy and security of information issues.

Our practical approach to privacy and data security challenges is what truly distinguishes our practice. We believe that it is our job to find innovative and realistic solutions for clients that balance legal compliance with the commercial realities of running their businesses.

We have been recognized by *Chambers* and *Legal 500* as one of the best domestic and global practices in this area. We were winners of *Chambers USA*’s award for excellence in the field of Privacy and Data Security 2008 and were named Privacy & Consumer Protection Practice Group of the Year by *Law360*. *Chambers Global* ranks the practice Tier 1 in its “Data Protection: Global” category. Clients have commented that our group comprises: “incredibly thoughtful, smart and responsive lawyers, who work seamlessly across different continents,” *Chambers Global*, and is “the best at giving practical advice by applying the law to the situation at issue,” *Legal 500 US*.

Our approach has made us the privacy counsel of choice for some of the world’s largest and best-known corporations, as well as a host of smaller organizations. Our skills are particularly valued by companies that operate in highly regulated sectors (such as financial services, healthcare, and pharmaceuticals), those with an online presence, those operating internationally and companies facing regulatory scrutiny or litigation. Our clients face multiple layers of regulation and appreciate the timely, knowledgeable, and realistic advice our attorneys are trained to provide.

We take a big picture view of how organizations handle information during its life cycle and help our clients find practical solutions to seemingly complex problems. From big data to cybersecurity to online behavior advertising, our lawyers work on cutting-edge issues that cover every aspect of privacy and data security.

**We Advise On:**

- U.S. and international privacy compliance
- Privacy litigation
- Regulatory investigations and inquiries
- Cross-border data transfers
- Cybersecurity and information security
“The work quality is exceptional, they are incredibly responsive, and they know about all the hottest issues in data privacy.”

– Chambers Global

The changing nature of technology has been a driving factor in data protection regulation in recent years, including issues such as the increased emphasis on technological means to secure data, how we use social media, user-generated content, the adoption of Cloud Computing, and sophisticated advertising and marketing techniques, including behavioral targeting. Our privacy and data security lawyers are as comfortable with technological innovation as they are with complex and evolving regulation. Because of wide experience with technology, we are at ease speaking with the general counsel, the chief privacy officer or the chief information officer regarding technical and non-technical issues relating to privacy and data security.

In addition to our transactional, regulatory and counseling practice, our lawyers are just as much at ease in the court room or with regulatory authorities in contentious situations. Our global team is able to help with virtually any privacy or data security issue anywhere in the world.

Resources

We offer important resources to support our clients in their privacy compliance and data security efforts.

- **Legal Resources:** The privacy team writes extensively on privacy and data security matters, including *Global Employee Privacy and Data Security Law*, setting out the U.S. and international legal landscape related to workplace privacy and data security; *Information Security and Privacy: A Guide to Federal and State Law and Compliance* and *Information Security and Privacy: A Guide to International Law and Compliance*, which compose a 4,300-page, three-volume treatise that examines all aspects of privacy and security laws, published by Thomson-West; and *The Law of Financial Privacy*, covering the Fair Credit Reporting Act, Financial Privacy Act, Bank Secrecy Act, and Internal Revenue Code requirements, including discussions of state financial privacy laws, use of technology, and use and protection of confidential information. The team has also written *Health Care Privacy and Security*, *West’s Corporate Counsel’s Primer on International Privacy and Security* and *Internet Marketing and Consumer Protection*. 


• **Privacy Library:** Our Privacy Library (www.mofoprivacy.com) is an online resource which provides links to privacy laws, regulations, reports, multilateral agreements, and government authorities of more than 90 countries around the world, including the United States. The Privacy Library is the most comprehensive collection of privacy laws and regulations ever assembled—the result of years of research and experience working with clients around the world.

• **MoFoNotes:** Morrison & Foerster provides content to Nymity (www.nymity.com) for its MoFoNotes product, a subscription-based database that helps organizations determine local compliance requirements in jurisdictions around the world, spot potential compliance issues, and simplify the development of global privacy approaches.
Clients value our “extensive network of attorneys around the world since privacy legal issues are becoming more global every day.”

- Legal 500 US
including preparing presentations to management, drafting communications, and establishing standard operating procedures and complaint handling procedures.

- **Global Health Care Company.** We advised on the adoption and implementation of a global framework agreement. We advised on the approach to consultations with works councils, drafted communications to management, human resources, sales, marketing and clinical research departments, conducted training for the procurement and legal functions globally, and prepared employee notice and consent forms. We also advised on and handled registration requirements in all EEA countries and relevant Latin-American countries, and handled all aspects of data transfer authorizations with regulatory authorities.
Articles and Alerts

Data Protection Masterclass:
Big Data and the Internet of Things – From Theory to Practice
The Internet of Things
Part 1: Brave New World

By Amy Collins, Adam J. Fleisher, D. Reed Freeman, Jr. and Alistair Maughan

The Internet of Things (IoT) is the network of everyday physical objects which surround us and that are increasingly being embedded with technology to enable those objects to collect and transmit data about their use and surroundings. TVs connected to the Internet and refrigerators connected to online delivery services are just the start of it. In the new world of the IoT, the possibilities are enormous, and the technology industry has so far only scratched the surface of what “machine-to-machine” (M2M) interconnectivity could achieve.

But the ingenuity and innovation which companies will apply to turn the IoT into practical reality is constrained by law and regulation. Existing issues may take on new dimensions and, as technologies combine, so will the legal consequences of those technologies.

In this Alert, we look at the prospects for the IoT. In a second Alert to be published shortly, we examine the likely legal and regulatory factors that will affect the development and growth of IoT technology and the markets that such technology will create.

BACKGROUND

The phrase “Internet of Things” was first coined in 1999 to mean the connection of everyday objects and devices to the Internet. The idea was that “If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory.”

But back in 1999, the technology required to make the IoT concept a reality was expensive, slow, reliant on dial-up Internet and limited by inadequate storage and processing power. Fast-forward 15 years, and the landscape in 2014 looks very different. All the key factors have converged to create the ideal conditions to harness the power of M2M connectivity: smartphones, Wi-Fi and broadband connectivity are now ubiquitous; storage capacity “in the cloud” is growing rapidly; sensor technology has developed sophistication while becoming cheap enough to deploy in almost any location; and data handling technology makes it possible to process large volumes of data in real time.

Coupled with improvements in the ability to process and analyse vast qualities of data – i.e., “Big Data” – the possible applications for Internet-connected devices are seemingly endless. Imagine stepping through your front door to find that your watch has downloaded to your computer details of your heart rate, pulse and vital signs, the thermostat has turned

---

1 http://www.rfidjournal.com/articles/view?4986
the heating up because of the cold weather outside, the bath has run automatically, and that later, while you sleep, your baby’s clothes monitor her breathing and heart rate while she sleeps. All of this technology is now available, although, in some cases, still at considerable cost: Wi-Fi-enabled Internet fridges currently cost a cool $3,700 (£2,300).

The uses of the IoT in a commercial context are also exceptionally wide-ranging: ATM data can be used to provide location-specific advertising to consumers via their smartphones, logistics companies can provide real-time parcel tracking services, and motor insurance providers can use telematics to monitor driving behaviour in order to charge tailored premiums.2 The IoT also looks set to revolutionise other sectors, including health care, with hospitals providing care via remote monitoring systems, and energy, with the advent of so-called “smart metering”.

As with previous waves of technology revolution, the consequences for business will be significant, in ways that are both foreseeable and unforeseeable. Just as the DVD destroyed the market for VHS movie rentals, the huge rise in Internet-enabled TVs seems likely to have the same effect on DVD sales as downloadable video-on-demand becomes ubiquitous. Other outcomes of connecting physical objects in the IoT are harder to predict: not only will existing functionality of separate objects be strengthened by M2M, but new functionalities will be created.

GOVERNMENT ATTENTION

The IoT looks set to be the focus of government attention. In a recent speech at Europe’s CeBIT tech conference, UK Prime Minister David Cameron announced that the British government would be spending an additional £45 million in funding for research in areas linked to the IoT, which, following a series of other funding announcements in this area, takes the total pot to £73 million. Mr Cameron stated: “I see the internet of things as a huge transformative development - a way of boosting productivity, of keeping us healthier, making transport more efficient, reducing energy needs, tackling climate change” and Sir Mark Walport, the UK government’s chief scientific adviser, is now expected to carry out a review into how these new technologies can be best exploited.

The EU has carried out extensive consultation on the development of the IoT, and the U.S. government, through the Federal Trade Commission, is also tracking the evolution of the market and technology in the sector.

CHALLENGES IN IMPLEMENTATION

The market for the IoT is still in its infancy and there are many challenges involved in deploying a solution. As with any eye-catching new technology, a lot of the hard work that goes into implementation often goes unnoticed.

In the case of the IoT, organizations will have to overcome significant initial hurdles in order to ensure that the solutions adopted are legally appropriate. In many cases, these include a number of the issues that are traditionally seen to be “outsourcing” type problems – e.g., implementing a scheme of contractual relationships necessary to implement and support the technology; choosing whether to partner with a service provider in order to develop and implement a particular solution; and determining whether and how to use an external agency to harness the necessary computing power to implement fully the solution.

One key internal issue that many organizations will also have to address is the question of who within the business is actually responsible for implementation of the IoT as a product solution. A lot of the tasks required for IoT implementation...
Client Alert

Implementation will fall within the traditional roles of a business’s ICT leaders, even though the solution itself may be customer-facing. As a result, technology leaders within businesses will need to be heavily involved in evaluating and developing solution requirements. This will continue the progression of the CIO role from overseeing internal enterprise architecture towards an outward-facing role.

Implementation of the IoT will also involve many of the operations parts of a business and this will need to be split appropriately within the architecture that the business employs. The question will be what solutions can be implemented as part of an overall scheme that is flexible enough to work with the types of devices and operating systems that a business has to deploy. Many of the end-to-end solutions that IoT requires involve the following key functions:

- **Device and infrastructure management platform.** The IoT requires operators to be able to operate software on devices remotely, without taking the network of sensors out of service. Clearly, where this is performed remotely, security of the device and infrastructure management platform will be crucial.

- **Data Filtering.** The IoT relies on sensors that produce vast amounts of data, but not all data will be relevant to any given application. Accordingly, a key challenge facing developers of IoT solutions is how to identify the thresholds and configurations to process only the data that is necessary for a specified purpose, and filter out the data that isn’t relevant.

- **Analytics Platform.** This is necessary to manage the huge volume of streamed data collected from remote sensors and devices and manipulate it in real time. This may well be integrated with an organisation’s approach to “big data” elsewhere in its business. But, whatever the platform (and whether internally provided or outsourced), it should be set up to work with data from different device types and locations and configure it in a way that is useable by the business.

- **Security.** If the IoT has a weakness, it’s security. Dealing with issues of privacy and data security is essential. Precautions against misuse if data need to be baked into IoT solutions from the outset.

- **Integration.** The efficiency and performance of any IoT solution will often depend on the connectors that enable applications to collect and analyse the data and engage in two way communication with the remote sensors where necessary.

The fact that technology is rapidly evolving and the relevant industry players are still changing means that future flexibility is also something that businesses need to focus on. Most large technology businesses have an established approach to the market and, while the first wave of solutions may well be focused on a particular application, businesses should invest wisely to ensure that the same sensor network and data infrastructure can be deployed to take on multiple applications.

The IoT has great potential to generate new sources of revenue, improve efficiencies and allow businesses to both increase profits and cut costs. While it is the internet-enabled products that catch the eye, it is longer term investment in the underlying technology infrastructure itself that is now required and which will ultimately pay dividends. The easy, media-friendly pin-up for the IoT may be the Internet-enabled refrigerator, but the reality is that the average consumer will replace his or her fridge no more than once per decade – and, most likely, not for improved functionality, just to keep the milk cold.
IOT BENEFICIARIES

Apart from humble consumers who might soon start to see practical changes to their daily lives as a result of the IoT, a range of companies in different sectors have already targeted the IoT as a driver of future sales.

If the trajectory of the IoT proceeds in the same way as other disruptive technology developments, the initial winners seem likely to be providers of infrastructure and data centre capacity, as well as microchip designers. Existing businesses with a strong data security element ought to have a key role in the IoT.

Companies that tailor their products to harness IoT capabilities and build in the key elements identified above will be the initial front-runners: so, for example, semiconductors need to continue to evolve in terms of size and power draw as well as enabling functionality to improve connectivity between sensor devices and the cloud, and the continued addition of new devices; infrastructure providers need to integrate their products for maximum flexibility while still ensuring significant levels of data security.

Consumer product manufacturers are perhaps the most obvious potential beneficiaries of the IoT as long as they can devise and roll-out IoT-enabled products whose functionality consumers want to pay for. But if history teaches us anything, it may be that, just as software giants became more valuable than the hardware sellers that capitalized on the first wave of the computing revolution decades ago (Microsoft vs IBM, anyone?), the long-term winners are less likely to be today’s major consumer product brands and more likely to be the companies that master and monetize the data to create entirely new markets.

Indeed, Google’s $3.2 billion purchase of connected thermostat producer Nest in January 2014 shows that the real market for IoT may take shape in ways that we cannot yet anticipate. That acquisition was less about a cool thermostat and more about disrupting the entire energy supply industry. If the Google and Nest combination can develop a product that proactively saves its users money on their home energy bills by juggling user and utility interaction and harnessing usage data, that puts Google in a strong position to continue its disintermediation efforts into a whole new sector.

LEGAL AND REGULATORY PROBLEMS

The opportunities of the IoT are great, but so are the challenges. The combination of technologies and data multiply the potential legal and regulatory issues.

In a follow-up Alert, we will assess the legal and regulatory factors that will affect the development and growth of IoT technology and help to shape the markets that such technology will create.

Contact:

Amy Collins  
(+44) 20 7920 4180  
acollins@mofo.com

Adam J. Fleisher  
(202) 887-8781  
a fleisher@mofo.com

D. Reed Freeman, Jr.  
(202) 887-6948  
rfreeman@mofo.com

Alistair Maughan  
(+44) 20 7920 4066  
amaghan@mofo.com
About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We’ve been included on The American Lawyer’s A-List for 10 straight years, and Fortune named us one of the “100 Best Companies to Work For.” Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.
The Internet of Things
Part 2: The Old Problem Squared

By Amy Collins, Adam J. Fleisher, D. Reed Freeman, Jr. and Alistair Maughan

Cisco estimates that some 25 billion devices will be connected in the Internet of Things (IoT) by 2015, and 50 billion by 2020. Analyst firm IDC makes an even bolder prediction: 212 billion connected devices by 2020. This massive increase in connectedness will drive a wave of innovation and could generate up to $19 trillion in savings over the next decade, according to Cisco’s estimates.

In the first part of this two part article, we looked at the development of, and practical challenges facing businesses implementing, IoT solutions. In this second part, we will look at the likely legal and regulatory issues associated with the IoT, especially from an EU and U.S. perspective.

THE ISSUES

In the new world of the IoT, the problem is, in many cases, the old problem squared. Contractually, the explosion of devices and platforms will throw up the need for a web of inter-dependent providers and alliances, with consequent issues such as liability, intellectual property ownership, and compliance with consumer protection regulations.

The IoT also raises a raft of data-related legal and ethical issues, associated primarily with the collection and use of the vast quantities of data processed as a result. The IoT will enable the creation and sharing of massive new reservoirs of data about individuals’ habits, behaviour and personal preferences, thereby reinforcing global society’s reliance on data, and making the laws and regulations which protect data privacy and limit data use even more fundamentally important.

Regulatory bodies, including the Federal Trade Commission (the “FTC”) in the United States and the European Commission (the “EU Commission”) in the European Union, are in particular turning their attention to the potential privacy and security issues that the IoT undoubtedly presents.

In 2013, the EU Commission published a report on the results of its public consultation on the IoT, along with a series of accompanying fact sheets (together, the “Report”), highlighting that “the development towards an IoT is likely to give rise to a number of ethical issues and debates in society, many of which have already surfaced in connection with the current Internet and ICT in general, such as loss of trust, violations of privacy, misuse of data, ambiguity of copyright, digital divide, identity theft, problems of control and of access to information and freedom of speech and expression. However, in IoT, many of these problems gain a new dimension in light of the increased complexity.”

Client Alert

At the top of the list of issues facing law and policy makers in this area are the following:

- **Loss of privacy and data protection.** The difficulties of complying with the principles of privacy and data protection, such as informed consent and data minimisation, are likely to grow considerably. The EU Commission has stated in its Report that “It can reasonably be forecast, that if IoT is not designed from the start to meet suitable detailed requirements that underpin the right of deletion, right to be forgotten, data portability, privacy and data protection principles, then we will face the problem of misuse of IoT systems and consumer detriment.”

- **Autonomous communication.** One of the most significant IoT-related data privacy risks stems from the fact that devices are able, and intended, to communicate with each other and transfer data autonomously. With applications operating in the background, individuals may not be aware of any processing taking place, and the ability for data subjects to exercise their data privacy/protection rights may therefore be substantially impaired.

- **Traceability and unlawful profiling.** Last year, researchers at Cambridge University demonstrated that incredibly accurate estimates of race, age, IQ, sexuality, personality, substance use and political views could be inferred from automated analysis of their Facebook “Likes” alone. Similarly, although the objects within the IoT might individually collect seemingly innocuous fragments of data, when that data is collated and analysed, it could potentially expose far more than intended by the individual to whom it relates, and indeed more than those Facebook Likes. The data collected, in combination with data from other sources, may reveal information on individuals’ habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling. This in turn increases the risk of authentication issues, failure of electronic identification and identity theft.

- **Malicious attacks.** The IoT provides hackers with more vulnerabilities to exploit and creates significant security risks. Such risks could take a variety of forms, depending on the nature of the data and device in question. In the context of e-health, the collection and rapid exchange of sensitive personal information in an interconnected and open environment not only increases risks in respect of patient confidentiality, but also has the far more alarming potential to endanger life. Take, for example, the remote programming of a heart pacemaker, or a drug dispenser configured to administer medication in response to a patient’s condition. A system failure or more sinister malicious attack on such device could have dire consequences. In the context of energy, hackers could target smart meters to cause major blackouts, and in the context of home security, it takes little imagination to contemplate the potential effects of a system failure or malicious attack. Such threats to security and privacy vary considerably and the breadth of challenges presented means that a one-size-fits-all approach to policy and/or regulation is unlikely to work.

- **Repurposing of data.** The risk that data may be used for purposes in addition to or other than those originally contemplated and specified by the data subject becomes even greater in the IoT. Repurposing of data may be contemplated even before data collection begins. For example, regulatory bodies, insurance companies and advertising agencies, among others, may seek access to data collected by others. Controls are needed to ensure that such data is only used in the manner consented to by the data subject. Whilst an individual

---

3 [http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html](http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html)
might be happy for his fridge to know how many pizzas he eats each week, he might be less comfortable if he knew that that information was being passed on to his health insurance provider.

- **User lock-in.** As is the case for existing technologies, the IoT increases the risk that consumers may become locked-in to a specific IoT service provider, thereby impeding their ability to retain control over their data and their right to move from one provider to another.

- **Applicable law.** With IoT devices, systems, users and service providers located in any number of jurisdictions, the global nature of the IoT means that various national laws may be applicable, each providing different levels of protection. This may give rise to questions of conflict, difficulties in enforcement and confusion among consumers.

**THE FUTURE REGULATORY LANDSCAPE**

Looking ahead, the question is, what approach should be taken by law and policy makers to address these issues?

In response to the EU Commission’s public consultation, a large number of industry players questioned the legitimacy and appropriateness of public intervention in an area which, although it has come a long way since 1999, is still arguably in its infancy. These stakeholders maintained that the existing legal framework, including data privacy, competition, safety and environmental legislation, is sufficient to protect end users’ interests, and inappropriate governance at this stage may stifle investment and innovation. Conversely, the majority of individual respondents argued that economic considerations should take a back seat to the fundamental issues of privacy and security. They contended that specific rules should be developed and enforced to protect end users and to control the development of IoT technologies and markets.

Keeping in mind (i) the international dimension of the IoT, (ii) the resulting need for interoperability, (iii) the importance of a harmonised internal market and (iv) the universality of the fundamental rights to privacy and data protection, the EU Commission commented that it would be inadvisable to allow divergence at a member state level of the law and methodologies in this area. That is, of course, a statement of the obvious.

But avoiding legal and regulatory fragmentation across key jurisdictions is a forlorn hope. Regulatory differences will occur, just as it has happened with Cloud, with data privacy and with many other regulated technologies. The truth is that governments just don’t act quickly enough to keep up with new technology, and don’t have the power or inclination to agree completely on harmonized legal and regulatory approaches to new technologies.

**EUROPE**

The EU’s draft Data Protection Regulation (the “Draft Regulation”), which is likely to be adopted in summer 2014, will go some way to provide the necessary harmonisation – at least within Europe. The Draft Regulation will replace the existing Data Protection Directive 95/46/EC and will have direct effect, not only to organisations established in the EU/EEA, but also to other organisations that collect and process EU/EEA residents’ personal data.\(^4\) Some of the measures that we might expect to see as a result of these developments are as follows:

---

\(^4\) For more on the changes proposed by the draft Regulation, see our January 2012 Alert A New Chapter in European Data Protection: Commissioner Reding Publishes Long-Awaited Draft Data Protection Regulation
Privacy by design and default. In its Report, the EU Commission noted that individuals’ privacy, data protection and security rights are often not considered at the outset of the design process, and it is unlikely that they will be properly addressed by the market without regulation. The Draft Regulation provides that, “having regard to the state of the art and the cost of implementation”, the data controller must, “both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures in such a way that the processing will ensure the protection of the rights of the data subject”. In addition, the data controller must “implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing, and are not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage”. In particular, those mechanisms must “ensure that by default, personal data are not made accessible to an indefinite number of individuals”.

Consent. In its Report, the EU Commission emphasised that mechanisms are needed to ensure that no unwanted processing of personal data takes place and that individuals are informed of the processing, its purposes, the identity of the processor and how to exercise their rights. The Draft Regulation defines consent as “any freely given, specific, informed and explicit indication” of an individual’s wishes, and can be expressed in the form of a statement or a clear affirmative action that signifies agreement to the processing. Tacit or implied consent could be valid: however, the preamble to the Draft Regulation confirms that silence or inactivity would not suffice. It remains to be seen exactly how these requirements will be met where applications in the IoT act autonomously and/or “behind the scenes”.

Measures based on profiling. As noted above, the IoT gives rise to serious concerns in terms of profiling and user traceability. The Draft Regulation sets out the circumstances in which such profiling, “which is based solely on automated processing intended to evaluate certain personal aspects…or to analyse or predict in particular the natural person’s performance at work, economic situation, location, health, personal preferences, reliability or behaviour”, would be considered lawful. This includes where the data subject has consented, or where, in the context of the performance of a contract, suitable measures to safeguard the data subjects’ legitimate interests have been adduced.

Privacy policies. In its Report, the EU Commission advised that privacy policies that can be pushed or built into IoT objects should be adopted, with appropriate mechanisms to ensure data privacy. It noted, however, that the technical challenge here is how to enable objects with limited processing power and/or memory to receive and respect such policies. Given the sheer number of IoT devices, the uniformity of such policies should also be considered.

Enforcement and sanction. The EU Commission also highlighted a need to strengthen and clarify the powers of data protection authorities to ensure consistent monitoring and enforcement of applicable law. Amongst other things, the Draft Regulation introduces significant sanctions for violations of data privacy obligations, including fines of up to 5% of annual worldwide turnover, or €100 million, whichever is greater. The Draft Regulation also extends the concept of mandatory personal data breach notifications to all areas of personal data processing.
Client Alert

In its Report, the EU Commission acknowledged that since the “IoT is a special case and more of a vision rather than a concrete technology, we understand that it is complex to properly define all the requirements yet”. Whilst the Draft Regulation goes some way to address the issues to which the IoT gives rise, it remains to be seen exactly how the law and policy in this area will develop as the IoT itself evolves.

UNITED STATES

On the other side of the Atlantic, privacy and data security in the IoT is also firmly on the agenda. Regulators in the United States – particularly the FTC – seem to be focused on the same privacy and security issues as their EU counterparts. In terms of how these concerns manifest in a regulatory context, the FTC is most likely going to rely upon its standard notice and choice framework on the privacy side, and its position that the lack of reasonable security measures to protect consumer data may be an unfair or deceptive act or practice under section 5 of the FTC Act. To that end, future FTC enforcement is most likely to focus in particular on two main areas when it comes to IoT: (1) providing notice and choice when a networked device is not consumer-facing; and (2) how to ensure that devices that are part of the IoT ensure reasonably data security.

We have various indicators of why the FTC will focus on these particular issues:

- **Workshop on the Internet of Things.** The FTC held a workshop examining privacy and security issues surrounding the IoT in November 2013. The workshop focused on those issues related to increased connectivity for consumers, both in the home (including home automation, smart home appliances and connected devices), and when consumers are on the move (including health and fitness devices, personal devices and cars). The FTC will publish a best practices report about the IoT at some time in 2014. The key themes articulated by the FTC at the workshop itself were: (1) the risks to consumer privacy from the collection, analysis, and unexpected uses of large amounts of data about consumers; (2) the possibility that traditional notice and consent frameworks will not be sufficient to inform consumers of how their personal data is being used; and (3) the data security risks of interconnected objects. In her opening remarks at the workshop, FTC Chairwoman Ramirez emphasized that “as the boundaries between the virtual and physical worlds disappear,” there still needs to be some way to give consumers notice and choice about the information collected about them, and how it is used, even if the device has no user interface.

- **TRENDnet Enforcement Action.** The FTC brought its first-ever IoT case in December 2013 against TRENDnet, the maker of a surveillance camera system with a range of uses from home security to baby monitoring. The company’s cameras had a faulty software configuration that left them open to online viewing, and in some instances listening, by anyone with the cameras’ Internet address. As a result, nearly 700 live camera feeds were accessed by a hacker. The FTC’s complaint alleged that the company’s failure to reasonably secure its cameras against unauthorized access was an unfair and deceptive act and practice under section 5 because the company represented it had reasonable security measures in place when it in fact did not. This type of case is fairly standard for an FTC data security case; what distinguishes it is that, as the FTC explained, the product involved falls under the IoT umbrella because it is an everyday product with interconnectivity to the Internet and other mobile devices.

---

• **FTC Commissioners’ speeches on the IoT.** Two FTC Commissioners have spoken recently about the policy and regulatory implications of the IoT, which gives some sense of future enforcement priorities and the contours of the regulatory framework:

  o In February 2014, Commissioner Julie Brill spoke on *The Internet of Things: Building Trust to Maximize Consumer Benefits*. Commissioner Brill tied the IoT to another major policy concern of the FTC – “big data.” She cited Cisco’s estimate that there will be 25 billion Internet-connected devices by 2015, and noted that by the end of this decade, 40% of data could come from connected devices. As a result, her main concern is that data from devices – that consumers might not even know are actually connected to the Internet – can be combined with existing troves of data to make it even easier to make sensitive predictions about consumers, such as those involving their sexual orientation, health conditions, religion and race.

  o In October 2013, Commissioner Maureen K. Ohlhausen spoke on *The Internet of Things and the FTC: Does Innovation Require Intervention?* While the Commissioner emphasized the potential privacy and data security risks posed by greater interconnectedness of devices, her remarks focused more on the transformative potential, and the human benefits, of the IoT. To that end, she sees the role of the FTC as ensuring that businesses have the freedom to experiment and innovate so that the benefits of this technological advance can be realized. Thus, while the FTC should use its traditional deception and unfairness authority to stop consumer harms arising from Internet-connected devices, the FTC should also focus on consumer tips and best practices relating to the IoT.

Finally, a number of U.S. states have proposed legislation on the 2014 docket that is intended to increase privacy protection for consumers. At a federal level, several bills are also in the process of going through Congress. These include the Black Box Privacy Protection Act⁶ (which would (a) prohibit the sale of automobiles equipped with event data recorders, unless consumers are able to control the recording of such data, and (b) require that any data so recorded would be considered the property of the vehicle owner) and the We are Watching You Act⁷ (which would provide for notification of consumers before a video service collects visual or aural information from the viewing area).

**CONCLUSION**

Given the tremendous growth of the Internet of Things, and the predictions that it will continue to grow exponentially, it is likely that the lawmakers and policymakers will play a considerable role in shaping the development of the IoT in the next few years.

The regulatory framework within which the IoT operates is an important factor to consider for technology companies seeking to harness the power of M2M connectivity. The key issue seems likely to be whether the regulators can (a) work fast enough to keep up with what the technology is capable of doing, and (b) whether law and policy in key market around the world is harmonized – at least in key parts – to ensure that the IoT is allowed to develop in a way supported by applicable laws, not handicapped by fragmented and contradictory legislation.

---


Client Alert

Businesses implementing M2M-based solutions will clearly need to examine their data privacy policies and approaches to data security in order to anticipate and meet the challenges presented by the IoT.

As noted above, Cisco is predicting that there will be 50 billion connected devices by 2020. Or, to put it another way, "Today there are more things connected to the Internet than there are people in the world. In the very near future, pretty much everything you can imagine will wake up." Numerous articles note the diversity of devices that can and will be connected in the near future, from cars to parking meters to home thermostats, which makes it seem as if we are at the beginning of an entirely new chapter in the history of the Internet.8

Contact:

Amy Collins  
(+44) 20 7920 4180  
acollins@mofo.com

Adam J. Fleisher  
(202) 887-8781  
afleisher@mofo.com

D. Reed Freeman, Jr.  
(202) 887-6948  
rfreeman@mofo.com

Alistair Maughan  
(+44) 20 7920 4066  
amaughan@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We’ve been included on The American Lawyer’s A-List for 10 straight years, and Fortune named us one of the “100 Best Companies to Work For.” Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.

---

**HOT TOPIC**

**HOT TOPIC: Wearables**

*E-Commerce Law & Policy* explores the opportunities and challenges presented by wearable technology, with perspectives from three jurisdictions around the world.

**UK**

Every footstep, heartbeat, ailment, location visited and event witnessed will be captured, stored and uploaded to the nefarious cloud - here lies the future of wearable tech. From Google Glass to elaborate health assessment clothing, wearable tech will be the next disruptive technology.

From a legal perspective, the potential problems are as vast as the opportunity is exciting. Intellectual property will be at greater risk of being copied and transferred, employers will need to be careful about employees covertly monitoring and recording every word and businesses will face the contradiction of having potential access to an array of data whilst having to address the ever increasing rise in laws to protect an individual’s privacy.

Legislators including the court will find themselves facing situations where the law fails to move at the same speed as the technology it is attempting to assess. Needless to say, lawyers will be busy assessing and reassessing policies, data permissions and procedures in order to protect their clients’ interests.

The development of wearable tech is exciting although we may all have to wait until the Cupertino giants at Apple introduce the iWatch before we all start craving for something without knowing why we really need it...

Garry Mackay Partner and Joint Chief Executive Officer Ashfords LLP, Bristol

g.mackay@ashfords.co.uk

**Belgium**

Google Glass gives its users hands-free access to a variety of smartphone online features. In its current form, Google Glass can, among other uses, pull information from the web, take photographs, record videos and provide navigation services. Applying current European data protection laws to such wearable technology raises many legal challenges, even though most laws exempt processing for domestic, household and recreational purposes from their scope. Fears of ubiquitous surveillance of non-users by users, whether through such recordings or through other applications currently being developed, have been raised.

Users will therefore have to understand (via a clear privacy policy) how to use Google Glass and where the sensitivities lie, not only in respect of themselves but also any non-users being filmed and recorded. The data protection regulators in the US, EU, Australia, Canada, Mexico and New Zealand have already indicated that Google, as a data controller, will have to address such issues which, most notably, relate to the privacy safeguards put in place by Google and app developers, the extent of the information collected by Google and shared by third parties (e.g., marketers, users’ employers, insurers and authorities), the ways in which and the purposes for which the information will be used, and sharing and security measures. Google has already indicated that it will not use the facial recognition function of Google Glass and that its privacy policy will address both users and non-users.

Karim Retzer Partner
Alja Polder De Zwart Associate
Morison & Foester, Brussels
KRetzer@mfo.com
APolderDeZwart@mfo.com

**Spain**

Wearables represent a business opportunity for e-commerce in the near future, but we should not lose track of the new challenges behind these devices.

On one hand, wearables can lead to the emergence of markets of new accessories to facilitate users’ lives with a high degree of customisation and functionality. These devices can also lead to new forms of technical innovation as well as the creation of new markets, but also involve a list of legal challenges.

As an example, what about protecting these devices in terms of design, patent registering and software rights as well as ensuring the right law is applied depending on the country where the devices are sold?

In my opinion, there is another, special challenge in this regard: simply finding the balance between the benefit wearables represent to users in terms of control and improvement through the use of these devices to aspects of their life: for e.g., health status or walking or sports habits, and how manufacturers deal with all that priceless private data. In this very case, more information means more business too.

Big data is the future but, is there any limit between privacy and doing business with it? Nowadays, the world’s legislation runs at a much slower rate compared to the speed markets move.

That is why we need lith and fast international legal instruments in order to regulate these situations in days to come. Again, here we are with a new challenge.

Vanesa Alarcón Partner & Co-Manager
Avatic Abogados, Spain
valarcon@avaticabogados.com

---

**SIGN UP FOR FREE EMAIL ALERTS**

E-Commerce Law & Policy provides a free email alert service. We send out free content, interviews and each month on the day of publication we send out a précis of all the articles in the new issue. To register visit [www.e-comlaw.com/ecip](http://www.e-comlaw.com/ecip) or email adelaide.pearce@e-comlaw.com