Legal Aspects of the Internet of Things
Richard Kemp
June 2017
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Para</th>
<th>Heading</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.</td>
<td>What is the Internet of Things?</td>
<td>1</td>
</tr>
<tr>
<td>2.</td>
<td>Why is it so important?</td>
<td>1</td>
</tr>
<tr>
<td>3.</td>
<td>How does the IoT fit into the 4th Industrial Revolution?</td>
<td>1</td>
</tr>
<tr>
<td>B.</td>
<td>PRACTICAL IOT LEGAL ISSUES</td>
<td>2</td>
</tr>
<tr>
<td>4.</td>
<td>Key practical IoT legal issues</td>
<td>2</td>
</tr>
<tr>
<td>5.</td>
<td>Key privacy and security challenges to be addressed in the IoT</td>
<td>3</td>
</tr>
<tr>
<td>C.</td>
<td>EU DATA PROTECTION LAW AND THE IOT</td>
<td>4</td>
</tr>
<tr>
<td>6.</td>
<td>How does EU data protection law address these challenges?</td>
<td>4</td>
</tr>
<tr>
<td>7.</td>
<td>Core IoT related definitions</td>
<td>4</td>
</tr>
<tr>
<td>8.</td>
<td>How do the data protection principles apply to the IoT?</td>
<td>5</td>
</tr>
<tr>
<td>9.</td>
<td>Legitimate processing</td>
<td>5</td>
</tr>
<tr>
<td>10.</td>
<td>Fairly and lawfully</td>
<td>6</td>
</tr>
<tr>
<td>11.</td>
<td>Purpose limitation</td>
<td>6</td>
</tr>
<tr>
<td>12.</td>
<td>Data minimisation</td>
<td>6</td>
</tr>
<tr>
<td>13.</td>
<td>Kept for no longer than is necessary</td>
<td>6</td>
</tr>
<tr>
<td>14.</td>
<td>Processing of sensitive data</td>
<td>6</td>
</tr>
<tr>
<td>15.</td>
<td>Transparency requirements</td>
<td>6</td>
</tr>
<tr>
<td>16.</td>
<td>Security requirements</td>
<td>6</td>
</tr>
<tr>
<td>17.</td>
<td>Data Subjects’ rights</td>
<td>6</td>
</tr>
<tr>
<td>18.</td>
<td>Terminal equipment</td>
<td>7</td>
</tr>
<tr>
<td>19.</td>
<td>What recommendations does the Opinion make?</td>
<td>7</td>
</tr>
<tr>
<td>20.</td>
<td>Recommendations for all stakeholders</td>
<td>7</td>
</tr>
<tr>
<td>21.</td>
<td>Recommendations for device manufacturers</td>
<td>7</td>
</tr>
<tr>
<td>22.</td>
<td>How will the GDPR change things?</td>
<td>8</td>
</tr>
<tr>
<td>D.</td>
<td>DIFFERENCES BETWEEN THE US AND EU APPROACHES</td>
<td>8</td>
</tr>
<tr>
<td>23.</td>
<td>What are the key differences between the US and EU approaches to privacy in the Internet of Things?</td>
<td>8</td>
</tr>
<tr>
<td>E.</td>
<td>CONCLUSION</td>
<td>9</td>
</tr>
<tr>
<td>24.</td>
<td>Conclusion</td>
<td>9</td>
</tr>
</tbody>
</table>
LEGAL ASPECTS OF THE INTERNET OF THINGS

A. INTRODUCTION

1. **What is the Internet of Things?** Whilst there is still no formally accepted definition, the Internet of things (IoT) is generally understood as everyday things, objects and devices that are connected to the Internet. The range of things is vast and increasing: watches, glasses and other wearables; health indicators; home automation like smart meters and connected lightbulbs, thermostats and fridges; right up to autonomous vehicles and connected cities. They include consumer facing devices as well as B2B devices to assist in manufacturing and supply chain management but generally don’t include smartphones, tablets, laptops and other computers themselves. What links all these things is their connection to the Internet through sensors to record, process, store and transfer data, whether they communicate between themselves, with computers or with people.

2. **Why is it so important?** In the early days of the PC, it was “chips with everything”. Now, in the era of the fourth industrial revolution, it’s “chips and sensors” with everything. Only a few years ago, there were more people in the world than things connected to the Internet. We’re just towards the start of this trend but on current estimates there are 25 billion things connected to the Internet at the moment and by 2020 this will rise to 50 billion. These new developments will bring enormous benefits to all of us in our daily lives as consumers in everything from healthcare to the home to transportation and insurance. And there will be benefits in the future that we can’t even begin to foresee at the moment. The rub is that much of the data that these connected devices generate and use will be personal data and some of that will be highly sensitive. And it’s really the issues about personal data and security that lie at the heart of the legal aspects of the Internet of things.

3. **How does the IoT fit into the 4th Industrial Revolution?** The fourth Industrial Revolution is a portmanteau term coined by DAVOS founder Klaus Schwab to describe the deep digital transformation of our lives that is just starting. These shifts cover everything from artificial intelligence and robotics to 3-D printing and ubiquitous computing. But many of them have at their heart the connected Internet of things –whether it’s wearables, the connected home, smart cities or driverless cars. All these changes centre on the cloud, big data and artificial intelligence. Cloud data centres are the engine room of the fourth Industrial Revolution. Volumes of digital data are currently doubling every 18 to 24 months – a bit like Moore’s law for data. Machine learning is the core component of AI and it works by crunching huge datasets to recognise patterns with increasing accuracy. Central to all these elements – the cloud, big data and AI - is the data produced by the sensors in the billions of devices that make up the IoT.
B. PRACTICAL IOT LEGAL ISSUES

4. Key practical IoT legal issues. For lawyers advising clients on projects related to the Internet of things, there’s a wide range of legal issues to be aware of. Commercially, the Internet of things will give rise to new patterns of business and business ecosystems, and the contracts underpinning them will need lawyering. Particular sectors like healthcare and financial services for example are likely to develop their own rules touching on IoT and at a more general level, consumer protection rules are also likely to be extended.

But it’s really in the areas of privacy, data protection and security that the most pressing legal issues arise. And there have been three reports over the last couple of years from government bodies on both sides of the Atlantic addressing practical legal issues around the Internet of things in these areas.

First, in the EU, the Article 29 Working Party is an independent advisory body on data protection and privacy set up under the current data protection Directive 95/46. In September 2014, it published an Opinion on the Internet of things (Working Paper 223) (‘Opinion’). The Opinion sets out the main issues, how the existing and future law should apply to the Internet of things and recommendations to stakeholders. Helpfully, it provides pointers looking ahead to May 2018 when the General Data Protection Regulation come into force.

Secondly, in January 2015 the US Federal Trade Commission published a staff report on the Internet of things called “privacy and security in the connected world” which covers similar ground from the US perspective.

Third, and most recently, NIST - the US National Institute of Standards and Technology - in November 2016 published a technical report from the engineering perspective on all aspects of security relating to the Internet of things.


5. **Key privacy and security challenges to be addressed in the IoT.** The privacy and security challenges that need to be addressed are clearly shown by a study from September 2016 by GPEN, the Global Privacy Enforcement Network, a grouping of national privacy authorities. The report found that about two thirds of devices surveyed failed to explain adequately to customers how their personal information was collected, used, stored and disclosed. In particular, almost three quarters failed to show it could be deleted off the device. And in just over one third of cases, the devices did not include include easily accessible contact details if customers had privacy concerns. It’s these failures to explain adequately and give notice that the regulators find particularly concerning. The Opinion unpacks these issues into six particular challenges:

(a) first, what it calls **lack of control and information asymmetry**: where device connectedness results in personal data generation, storage and communication over which the user has no control.

(b) secondly, **quality of user consent**: the user’s consent to the processing of data carried out by IoT devices must be informed and the standard will rise when the GDPR comes in next year. In many cases the user will not be aware of the data processing carried out by a particular device and in these cases consent cannot be relied on under EU law as it is not properly informed.

(c) third, **secondary use and repurposing**: where big data analysis techniques may lead to device data obtained for one purpose being used for a quite different purpose for which no consent has been given.

(d) next, **aggregation of data** from different devices may reveal specific aspects of individuals’ habits, behaviours and preferences in an unduly intrusive manner.

(e) fifth, limitations on the possibility to **remain anonymous** when using services.

(f) finally, **security risks**: physical constraints, for example balancing battery efficiency and device security, may lead to manufacturers reducing security – the implementation of confidentiality, integrity and availability measures – to reduce costs.

---

C. EU DATA PROTECTION LAW AND THE IOT

6. How does EU data protection law address these challenges? The Opinion confirms that EU data protection law applies to the Internet of things and then applies these rules to the IOT world, looking at:

- core definitions; [paragraph 7];
- how the data protection principles apply to the Internet of things [paragraphs 8 to 14];
- transparency requirements [paragraph 15];
- security requirements [paragraph 16];
- data subject rights [paragraph 17]; and
- certain rules from the e-privacy directive about terminal equipment [paragraph 18].

7. Core IoT related definitions. The Opinion gives a broad definition to IoT devices as “all objects that are used to collect and further process the individual’s data in the context of the provision of services in the IoT”. It states EU data protection law will apply in respect of those devices even where data controller is outside the European Union provided that the device has been used within the EU.

Personal data is of course broadly information from which an individual may be identified and the Opinion states that even data intended to be processed after the implementation of techniques like pseudonymisation may need to be considered as personal data because of the risks of re-identification – where data from one device aggregated with one or more others enables an individual to be identified, even though that individual could not be identified from one device alone.

The Opinion provides a helpful discussion of the various stakeholders in IoT ecosystems and how they may qualify as data controllers, a core building block of EU data protection law as a person who by himself or with others determines the purposes and means of processing personal data. So, device manufacturers, social media platforms, third-party application developers, data hosting providers and insurers may all be data controllers in using data generated by IoT devices for specific purposes that they determine.

Users of IoT devices will qualify as data subjects under EU law. An important point is that ownership of a particular IoT device is not a factor that is relevant as to whether someone is a data subject – the key thing is that if the device processes personal data the individual concerned will be the data subject.
8. **How do the data protection principles apply to the IoT?** Where an IoT stakeholder is a data controller the Opinion calls out a number specific obligations that apply. These correspond in the IoT world to compliance with the data protection principles.

9. **Legitimate processing.** The Opinion discusses the three ways set out in Article 7 of the Data Protection Directive for processing personal data to be legitimate. Essentially, these are:

   - that the data subject **consented**;
   - that the **processing is necessary for the performance of the contract** to which the data subject is a party; and
   - where the **processing is necessary for the purposes of the legitimate interests of the data controller** except where inconsistent with the fundamental rights of the data subject.

   **Consent** is a thorny issue in data protection terms and getting thornier. The Information Commissioner’s Office (‘ICO’), the UK regulator, has recently consulted on its draft guidance on consent, and we await the finalised guidance. The draft guidance notes that the GDPR will set a high standard for consent. It means offering individuals genuine choice and control, and requires a positive opt-in and a very clear and specific evidenced statement of consent. Importantly, data controllers must make it easy for people to withdraw consent and tell them how. Relying on consent in the IoT context is therefore likely to become more difficult.

   The second way is that the processing must be **necessary for the performance of the contract**. Here, quotes necessary has tended to be interpreted narrowly and to require a direct and objective link between the processing itself and the purpose of expected contractual performance.

   The third way is even more restrictive and the Opinion refers to the **Google Spain** case to say that economic interests are not by themselves legitimate interests.

---


8 Judgment of the European Court of Justice (Grand Chamber), 13 May 2014, Case C-131/12.
10. **Fairly and lawfully.** Once the legitimate basis for the processing has been established, personal data should then be collected and processed consistently with the other data protection principles. This means data should be collected and processed fairly and lawfully – the individual should be aware that this is going on, for example.

11. **Purpose limitation.** The purpose limitation principle means that the data can only be collected for specified, explicit and legitimate purposes. These purposes must be defined before processing takes place which in turn means that IoT stakeholders must have a good overview of their business case before they start collecting personal data.

12. **Data minimisation.** The personal data collected must be strictly necessary for the specific purpose concerned – the data minimisation principle. As the opinion says (at page 16), necessary data should not be collected and stored “just in case” or because “it might be useful later”.

13. **Kept for no longer than is necessary.** Finally, personal data should be kept for no longer than is necessary. This test must be met by each IoT stakeholder for their specific service. For example, the Opinion says (at page 17) that personal data communicated by a user when subscribing to a specific service on the IoT should be deleted as soon as the user ends the subscription. Similarly, account information deleted by the user should not be retained.

14. **Processing of sensitive data.** Sensitive data about an individual’s health, for example is subject to a higher standard in the IoT as in other areas effectively requiring the user’s explicit consent.

15. **Transparency requirements.** Data controllers must meet certain transparency requirements – they must give notice to data users of the identity of the controller, the purposes of the processing, the recipients of the data and the existence of data users rights.

16. **Security requirements.** As in other areas of data protection law the controller must implement appropriate technical and organisational measures to protect personal data – they must keep the data secure. This means that any IoT stakeholder who is a data controller remains fully responsible for the security of the data processing. This is as much a technical as a legal issue. The US NIST paper on systems security engineering puts considerable reliance on an international standard, ISO 15288 on systems and software engineering. It is likely that this standard will emerge as the benchmark for determining compliance in the IoT world with the data protection security requirement.

17. **Data subjects’ rights.** IoT data controllers must respect the rights of the data subject in the same way as other data controllers. So, data subjects must be able to obtain details of the data that the controller holds about them. And data subject must be able to withdraw consent previously given and to object to the processing of data relating to them.

---

9 [https://www.iso.org/standard/63711.html](https://www.iso.org/standard/63711.html)
18. **Terminal equipment.** Where an IoT stakeholder stores or accesses information already stored on an IoT device, that device will qualify as “terminal equipment” under the e-Privacy directive\(^\text{10}\). There is a further requirement here for consent by the subscriber to that storage or access. This consent requirement primarily concerns the device manufacturer but will also be relevant for anyone else who wants access to the aggregated raw data.

19. **What recommendations does the Opinion make?** Having gone through the legal requirements, the opinion then lists a number of recommendations to help data controllers in the IoT ecosystem comply with their legal obligations.

20. **Recommendations for all stakeholders.** The Opinion first makes a number of recommendations that apply to all stakeholders:

   - *Privacy impact assessments*\(^\text{11}\) should be carried out before the launch of any new application;

   - *raw data should be deleted* as soon as data required for processing has been extracted;

   - the principles of *Privacy by Design* and *Privacy by Default* should be applied. This means as the names suggest that data protection compliance should be baked in to the design of the product or service and that it should default to compliance with privacy rules;

   - using the now fashionable tagline, *data users and subjects should be “in control”* – they should be able to determine how their data is used;

   - information about the processing should be given in a *user-friendly manner*; and

   - *consent must be explicit, informed and freely given* and users should have the opportunity to withdraw it.

21. **Recommendations for device manufacturers.** Device manufacturers should:

   - give information to users about the *types of data* that are collected, the types of data the sensors receive and how they will be processed and combined;

---


• inform all stakeholders as soon as the data subject withdraws consent;
• disable wireless interfaces when not in use;
• provides tools to enable the editing of data locally before it is transferred to the data controller;
• give users a right of access to data and the ability to export data;
• notify users when security vulnerabilities are discovered;
• enable devices to distinguish between different users; and
• work with standardisation bodies to develop common protocols.

The opinion makes (at pages 23 and 24) similar specific recommendations from other IoT eco-system participants like application developers, social platforms.

22. How will the GDPR change things? When it comes in in May 2018, the GDPR will significantly broaden and deepen the range of obligations that data controllers must comply with. These apply in the IoT area as elsewhere. The Opinion has been helpful in looking ahead to when the GDPR is in force, particularly in relation to stressing the need for a structured approach as in the case of privacy impact assessments, privacy by design and privacy by default. However the new requirements will make life more exacting in data protection terms for IoT participants.

Importantly, data processors – who process personal data on the instructions of a data controller – are outside of the net caught by the Data Protection Directive at the moment but inside it when the GDPR comes into force. This means that for the first time they will have a range of directly enforceable duties which they will need to comply with.

IoT eco-participants will also need to be mindful of include the risk of penalties for breach that could amount to 4% of worldwide turnover; tougher and more granular consent requirements, as we have seen; rules on data breach notification; profiling restrictions and the right to be forgotten.

D. DIFFERENCES BETWEEN THE US AND EU APPROACHES

23. What are the key differences between the US and EU approaches to privacy in the Internet of Things? Interestingly, as we have all got used – with safe harbor and the privacy shield – to the differences between US and EU privacy law, the EU Article 29 Working Party Opinion from 2014 and the US FTC IoT Staff Report from January 2015 have more things in common than things that separate them.
The FTC report was released against a backdrop of active prosecutions against IoT device makers for privacy and security breaches. It sets out a number of recommendations for device manufacturers who should:

- adopt what the FTC calls a security by design approach;
- carry out a training and awareness campaign for employees to ensure that security is managed at all levels within the organisation;
- ensure that third party service providers are required to follow the same security standards; and
- adopt a “defence in depth” strategy for security risks – i.e. to ensure that there are multiple layers of security to combat a particular risk.

E. CONCLUSION

24. Conclusion. The IoT will continue to be a top priority for regulators in the data protection and security areas. Compliance with the broadening and deepening requirements of data protection law will continue equally to be high on the agenda of all participants in the IoT ecosystem.

Richard Kemp
Kemp IT Law, London
June 2017
richard.kemp@kempitlaw.com