Are banks ready for the Internet of Things revolution?

Part 2: New legal issues created by the Internet of Things

16 OCT 2017
By: Giulio Coraggio

As with almost any change in the way businesses are run, the Internet of Things will lead to new legal issues. Here are key issues we are already seeing:

1. Privacy issues become bigger

Banks have always processed large amounts of data and had to face privacy issues. However, Internet of Things technologies will raise the stakes because:

- data will no longer be collected only from bank accounts, home banking technologies and branches, but from devices, cars or factories and
- data will be used not only to ensure the proper performance of financial transactions, but to provide services and make savings. It will also be shared with third parties.

This IoT-led period of transformation is already taking place. Meanwhile, the European Union's General Data Protection Regulation is set to come into force, raising the risks posed to enterprises.

Among other things, the GDPR will:

1. increase fines to up to 4 percent of the global turnover of the breaching entity
2. lead to higher risks of claims from customers: the Regulation introduces the principle of accountability, placing the burden of proving privacy compliance on the investigated party
3. generate a higher risk of claims from shareholders because of the size of potential fines and claims and
4. retain the existing criminal sanctions and orders for deletion of data.

Furthermore, the current draft of the EU's ePrivacy Regulation extends its scope to machine-to-machine communications; therefore, the scope of privacy rules may also apply to the processing of non-personal data to pure Industry 4.0 technologies.

Privacy compliance will no longer rely just on the proper arrangement of documents, but will depend on:

1. the ability to map and control data
2. the implementation of organizational procedures to ensure the proper processing of personal data both internally and with reference to third-party suppliers/agents and
3. the adoption of technologies able to minimize the risk of illegal access to data and identify unlawful treatments so they can be promptly addressed.

2. Data anonymization to better exploit data

A possible solution to minimize privacy-related restrictions is to implement anonymization or encryption solutions. The tricky element in this context is figuring out how to ensure that the anonymization/encryption does not at the same time strip away the data's valuable information.

3. Increased threat of cyberattack

Collecting more data from different sources will inevitably increase the risk of a cyberattack. Like any technologies, the IoT cannot be 100 percent secure.

Companies need to put in place measures to limit the risk of cyberattacks and, should such attacks occur, should be able to prove they have complied with due diligence principles. These measures include, among others:

1. the adoption of a cyber-risk policy, including a procedure to handle a data breach
2. a cyber-risk insurance policy
3. the implementation of a security and "privacy by design" approach
4. the appointment of a data protection officer.

4. Agreements with third parties need to be "adequately" managed

Given the size of privacy and cyber-risks, agreements with third parties that provide services as well as with those that intend to exploit data shall be drafted in a way that:

- ensures the minimization of risks deriving from third parties, but at the same time
- guarantees that in case of a data breach or unlawful processing of personal data, uncapped indemnity claims can be brought against banks.

5. Different legal basis shall be considered to ensure data ownership

The European Commission is considering a variety of options to protect IoT data and its ownership. The most viable routes currently being considered are the following:

1. **data is linked to the device**. This is more a factual status than a legal basis, but technology providers tend to structure their platforms/devices so that they keep control of processed data
2. **data can be protected under copyright law**, but this would require an "intellectual effort" in the data's collection/organization/analysis
3. **data can rely on the European database sui generis right**, which is broader than copyright
4. **data can be considered trade secrets** or can be protected under antitrust regulations, making its exploitation an

unfair competition conduct.

6. Data can be "stolen" through the data portability right

The new data portability right introduced by the EU General Data Protection Regulation is both a resource and a risk for a business. For more information on DLA Piper's view of the key changes to the current data protection framework see here.

7. Data needs to be used

Currently, a number of companies are collecting data without actually using it, effectively just creating their own database. Such conduct would not only be in breach of privacy regulations in certain jurisdictions, but also might lead to allegations of misleading advertising if customers have been led to believe they will receive tangible benefits by providing their data.

Finally

Many interesting opportunities will arise for financial services through Internet of Things technologies. The challenge will be to properly exploit them for competitive advantage in a manner that mitigates cyber-risk and legal risk. Learn more by contacting the author.

For more information about issues raised in this article, please get in touch with the author below.

Keep an eye out for our upcoming TechLaw Series events which we will be regularly updating here.

Read Part 1: The rise of the Bank of Things

AUTHORS

Giulio Coraggio
Partner
Milan | T: +39 02 806181
giulio.coraggio@dlapiper.com