TECH LAW BRIEFING

Security issues with Internet of Things ("IoT") products

According to a study by eco ("Verband der Internetwirtschaft e.V." – "Association of the Internet Industry"), the German IoT market will generate revenues of around EUR 16.8 billion in 2022. This would mean a doubling within five years and a growth of around 19 % per year. Germany is among the world's largest industry 4.0 markets (especially in the automotive industry, but also in mechanical and plant engineering).[1]

IoT devices often raise questions of liability and IT security, as well as questions of data protection. In recent years, IT security specialists showed how easily they can access some of those devices to gain control over them or infiltrate the network the devices are connected to.[2]

DATA PROTECTION

IoT products generally offer a broad variety of sources for personal data. The data collected by IoT products can roughly be divided into sensor data (biometric data, video cameras, microphones, etc.) and user data (data related to user accounts or other data that can somehow be related to an individual person). Due to the sheer mass of personal data that can and most likely will be collected by IoT products, the principle of data economy presents a challenge for the compliance of IoT products. To prevent a product from being inadmissible under data protection law, manufacturers should seek ways to make their products compliant with this fundamental data protection principle. Possible methods to achieve this could be the early deletion of personal data, the preference of a local data processing over cloud processing (Fog Computing should be preferred over Cloud solutions) and anonymization as well as pseudonymization of personal data.

Another obstacle to compliance with data protection law could be the obtaining of effective user consents. A given consent might be deemed unlawful if its scope does not cover every aspect of the data use of the IoT product. This is often caused by the fact that IoT systems can be very complex and confusing for the average consumer. This problem could be avoided through a clear and comprehensive communication of the functionality of the IoT device.

With the constant further development of IoT products and their increasing data protection relevance, the demands placed on the technical and organizational measures are also increasing. For example, IT security must be ensured to a particularly high degree for very sensitive data (e.g. health-relevant data from fitness wristbands). As always, the principles of "privacy by design" and "privacy by default" must be observed.

LIABILITY

The European Product Liability Directive[3] is currently a legal grey area, since it only covers physical goods. It is under an ongoing broad evaluation by the European Commission whether its rules and overall functioning remain appropriate for new technologies such as IoT products.[4] As an interim result, the European Commission recently concluded that the current legal framework on product liability contains shortcomings for victims suffering damages caused by complex IoT products compared to damages resulting from traditional technologies.[5] Consequently, the Commission considers amendments to the existing legal stipulations, such as adapting the burden of proof.[6]

For liability issues related to the manufacture of IoT products, a closer look at the German Product Liability Act is required. It states that the manufacturer is liable without fault if the defect in a product kills someone, injures their body or health or damages an item. The Product Liability Act covers movable items including embedded software (some voices also consider independent software itself a product in the sense of this law). It is therefore applicable to most IoT products. The manufacturer may be able to evade liability if he can prove that the damage could not have been prevented despite using state of the art protection measures. In these cases the damage has to be based on unpredictable circumstances. There are also voices that argue that the consumer should not bear the risk for knowledge gaps in security of new technologies.[7] However, liability could be reduced where the injured party does not perform security relevant updates, since this could be regarded as contributory negligence.[8] Moreover, manufacturers may be able to limit their liability in certain areas if they comply with DIN SPEC 27072[9] (Information Technology – IoT capable devices – Minimum requirements for Information security) and the BSI catalogue on security requirements for IT systems.[10]

An upcoming problem in the area of product liability is the distinction between manufacturers of different parts of the IoT product. In order

[1] https://www.eco.de/presse/studie-von-eco-und-adl-industrial-iot-umsaetze-wachsen-bis-2022-jaehrlich-rund-19-prozent/
[2] E.g. https://www.golem.de/news/smart-home-wenn-die-lampe-zum-trojaner-wird-1901-138712-2.html
[3] Council Directive 85/374/EEC.
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN
[5] https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf, p. 12ff.
[6] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, p. 15.
[7] de Meeus: The Product Liability Directive at the Age of the Digital Industrial Revolution: Fit for Innovation?, EuCML 2019, 149, 152.
[8] https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064
[9] https://www.din.de/de/din-und-seine-partner/presse/mitteilungen/din-spec-27072-mehr-sicherheit-im-smart-home-330088.
[10] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Cyber-Angriffe_durch_IoT-Botnetze_25102016.html.

BEITEN BURKHARDT

to improve this situation, it could be advisable for manufacturers to describe their respective service as precisely as possible in order to allow a clear separation of responsibilities.

In the context of product liability, the manufacturer must, among other things, comply with product monitoring obligations. These may conflict with data protection law and require a precise examination of whether the specific product monitoring obligation in each case can justify the use of personal data. A possible justification could be that the data collection is necessary for the provision of security- or functionality-related updates. This would be in line with the recommendations of the "International Working Group on Data Protection in Telecommunications" concerning the updating of firmware of embedded systems in the Internet of Things.[11]

Apart from this, the EU directives 2019/770 and 2019/771 contain the obligation of the manufacturer to keep the content in conformity with the contract by means of updates (relevant for security and functionality), not only in cases of continuous obligations but also in cases of one-time purchases.[12] Concerning a continuing obligation, the obligation will exist during the whole term of the contract. Regarding one-time purchases it shall last as long as the buyer can reasonably expect to be provided with updates. IoT products might therefore oblige the manufacturer to provide updates for the duration of the average "lifetime" of a certain product. According to a rule of doubt, the obligation shall at least exist as long as the manufacturer is liable for defects (i.e. two years).[13] The directives have to be implemented by the EU member states before the 1st of July 2021.

IoT users can currently only be held liable if they are at fault. Due to the complexity and unpredictability of modern IT systems and therefore very low control obligations for the user, this case will hardly arise. The possibility of a contractual shift of risks and liabilities to consumers seems unlikely as well. The average consumer will regularly not be aware of the potential risks he or she assumes with his or her acceptance.

In the case of sellers of IoT products who are not themselves manufacturers the general warranty claims must be taken into account, which may, for example, result from a lack of IT security or a system failure. In case of doubt, however, they should be less obligated than the manufacturers themselves, so that their liability risk should be somewhat lower or at least easier to calculate.

Susanne Klein
Lawyer | LL.M. | Licensed Specialist for Information Technology Law
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Frankfurt am Main

Peter Tzschentke
Lawyer
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Frankfurt am Main

[11] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_Firmware_Updates-en.pdf.

[12] Art. 8 (2) Council Directive 2019/771/EC, Art. 7 (3) Council Directive 2019/771/EC.

[13] Recital (47) Council Directive 2019/770/EC, Recital (31) Council Directive 2019/771/EC.

Imprint

This publication is issued by
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33 | D-80339 Munich
Registered under HR B 155350 at the Regional Court Munich/VAT Reg. No.: DE811218811

For more information see:
https://www.beiten-burkhardt.com/en/imprint

EDITOR IN CHARGE
Dr Andreas Lober | Lawyer | Partner

YOUR CONTACTS

DUSSELDORF
Cecilienallee 7 | 40474 Dusseldorf
Mathias Zimmer-Goertz
Tel.: +49 211 518989-144 | Mathias.Zimmer-Goertz@bblaw.com

FRANKFURT AM MAIN
Mainzer Landstrasse 36 | 60325 Frankfurt am Main
Dr Andreas Lober
Tel.: +49 69 756095-582 | Andreas.Lober@bblaw.com

MUNICH
Ganghoferstrasse 33 | 80339 Munich
Dr Axel von Walter
Tel.: +49 89 35065-1321 | Axel.Walter@bblaw.com