Int. Cybersecur. Law Rev. (2020) 1:27–37
https://doi.org/10.1365/s43439-020-00006-3

Regulation of Internet-of-Things cybersecurity in Europe and Germany as exemplified by devices for children

Stefan Hessel · Andreas Rebmann

Received: 13 February 2020 / Accepted: 13 March 2020 / Published online: 23 September 2020

Abstract IoT devices are omnipresent in children's rooms. At the same time these devices and their infrastructure have become notorious for security flaws. The following paper analyses current and future legal reglementation and IT security measures to protect children as an especially vulnerable group.

Keywords Connected toys · Cybersecurity Act · Toy Safety Directive · Radio Equipment Directive (RED) · General Data Protection Regulation (GDPR)

1 Introduction

The digitalisation of our society is affecting our entire living environment at an increasing rate. Within the framework of this, more and more data on our environment, but also on ourselves, is being processed. This is no longer done exclusively by conventional computers but by Internet-of-Things (IoT) devices. However, these are not only used in a smart home or in applications for adults but have also found their way into the lives of children. This is reflected not only in very positive market forecasts [1] but also in Mattel's ultimately failed attempt to market a Smart Home Hub for children [2]. However, children are considered a particularly vulnerable group which enjoys special protection under Article 24 of the EU Charter of Fundamental Rights and Article 6 of the German constitution. This gives rise to the question of how secure the devices are from a technical point of view and which

S. Hessel (✉)
reuschlaw Legal Consultants, Stengelstraße 1, 66117 Saarbrücken, Germany
E-Mail: stefan.hessel@reuschlaw.de

S. Hessel · A. Rebmann
Universität des Saarlandes, Campus, 66123 Saarbrücken, Germany
E-Mail: andreas.rebmann@uni-saarland.de

legal requirements apply to the IT security of devices for children in particular but also to IoT devices in general.

2 Technical background

The concept of ubiquitous computing describes the shift from computers being located in a few common spots such as desktops and workplaces to being part of everyday objects formerly not associated with technology-equipped products [3]. IoT devices are part of this phenomenon as more and more everyday objects become connected to networks and the internet [4]. This includes cars, so-called wearables and video surveillance but also products specifically designed for children, such as toys and learning devices. As the number of internet-connected devices grows rapidly, the number of devices vulnerable to attacks and used in a malicious way increases equally. IoT devices for children can largely be grouped into four categories: connected toys, kids' smart watches, tablets for children and monitoring devices, serving multiple purposes [5]. In addition to the common IT security problems concerning all computer devices, those specifically targeting children must deal with additional issues, as children have a different approach to handling devices while requiring a special level of protection [6].

2.1 Connected toys

Connected toys are toys—such as teddies, dolls or even pacifiers—that are either directly connected to an online platform or via an additional device, oftentimes a smartphone with a specific app installed. Connected toys therefore require a Wi-Fi or Bluetooth connection in order to transfer data to and from the device. The kind of data transferred depends on the toy and its features and purpose. Many of the connected toys are built to interact with their users. Mattel's "Hello Barbie" and Vivid's "My friend Cayla" were designed to record children's voices through an internal microphone and give appropriate answers via an integrated speaker. Through an active Wi-Fi (Hello Barbie) or Bluetooth (My friend Cayla) connection the voice recordings were transferred to a smartphone and then sent to the manufacturer's server. On the server the voice recording would undergo a speech to text algorithm whose results would then be sent back to the app. The app redirects the question to Wikipedia and an appropriate answer would be sent back to the toy which replies to the children's input. Other devices use cameras with image recognition technology, as did Mattel's "Smart Toy Bear", which also featured speech recognition and was discontinued in 2019.

While digital assistants and smart speakers such as Amazon Alexa, Google Home and Apple's Siri, which are rising in popularity [7], are largely confronted when it comes to privacy issues, similar children's devices keep drawing media attention associated with data security risks.

Data processing such as voice recognition usually does not take place on the device itself but rather on a company's server offering much higher computing power and capacities. In the past such cloud servers storing audio data, their transcripts

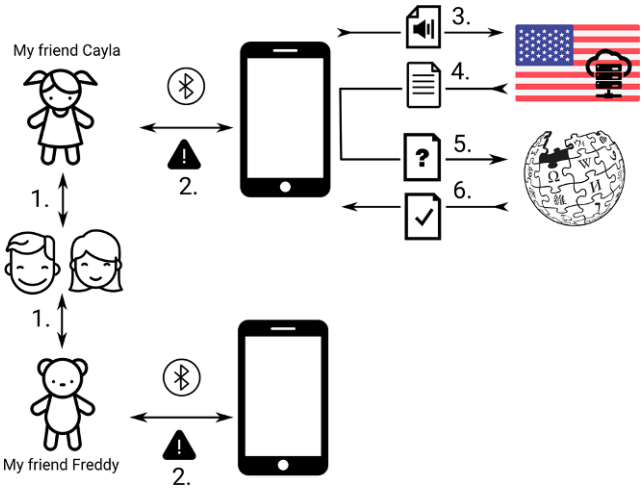

Fig. 1 While "My friend Cayla" sends data to US servers, data processing with "My friend Freddy" occurs on the user's smartphone. *1* Dialogue of the child with the toy, *2* unsecured Bluetooth connection, *3* voice transmission to the USA, *4* return of a text file, *5* search at Wikipedia, *6* output of the answer. (Image: Stefan Hessel, Icons: Freepik from Flaticon, Creative Commons BY 3.0)

and often a user's account information have been attacked and personal data of children have been downloaded in large quantities [8]. In the 2015 VTech hack profile information of more than six million children was stolen as well as voice recordings of more than 1.2 million users [8]. But not only the platforms but the devices themselves have been credited with lacking security measures and therefore posing a risk to children. In 2016 the Norwegian Consumer Council looked into privacy and security measures of connected toys and discovered major IT security flaws in several of them [9]. The connected toy doll "My friend Cayla" was equipped with a Bluetooth microphone and speaker, making it essentially a Bluetooth headset inside a doll [10]. Users could connect the doll's Bluetooth device to the manufacturer's smartphone app in order to use features requiring a network connection, such as interactive conversations and directing questions at the doll and getting responses. The Bluetooth devices did not use any form of authentication to connect to external devices, enabling any Bluetooth equipped device within the toy's range to use the microphone and speaker inside the doll. This security issue did not only enable anyone to talk to children through the doll, it also worked as a spying tool, recording anything around the doll and sending it to the connected devices. The latter led the German Federal Network Agency (BNetzA) to take "My friend Cayla" off the market and making its possession in Germany illegal due to Article 90 of the German Telecommunications Act (TKG) [11]. The teddy "My friend Freddy" works similarly but does not send data to external servers. Since data processing occurs only on the smartphone, "My friend Freddy" is not affected by article 90 TKG.

Connected toys that can interact with children pose another problem that is not connected to privacy or IT security: surreptitious advertising targeted to children.

"My friend Cayla" has been criticized by several organizations, among them the European Consumer Organization BEUC, for advertising candy products [12] and toy stores [13] to their minor users (Fig. 1).

2.2 Children's smart watches

Just like regular smart watches, those specifically advertised to children grow in popularity. In 2018 more smart watches designed for children were sold in China than regular smart watches [14]. Alongside a special and often colorful design, smart watches for children often differ in functions from those marketed to adults. Like connected toys, several smart watches have been found to have major security flaws that enable attackers to spy on children wearing the devices. In 2017 the Norwegian Consumer Council "*Forbrukerradet*" investigated numerous children's smart watches and found several of them to be easily vulnerable to hacking [15]. The watches could remotely be instructed to make a call to any phone number given by the attacker, enabling them to listen in on any communication made within the vicinity of the watch without the children's knowledge. In one case the Norwegian Consumer Council found this to be an advertised feature for concerned parents rather than a security flaw. In 2019 the European Commission warned about similar flaws in some smart watches for children [16]. Unlike most connected toys, children's smart watches are additionally equipped with GPS trackers, enabling parents to locate their children. This main feature can easily be used in many watches in a malicious way, as watches fail to require proper authentication to connect another device, as the *Forbrukerradet* showed [17]. In early 2020 a bug in Chinese manufacturer TCL's app for their "Movetime Family Watch" was discovered, enabling users to randomly access any other user's account information, including location and voice messages [18]. Additionally, researchers found data sent to servers to be insufficiently or not at all encrypted, making it possible to secretly track a child's position. The servers in question were found to be a security flaw themselves. Many of them belong to third parties and are located in East Asia or North America [19]. These third party servers as well as servers of the service providers were found to store large amounts of user information from account names, phone numbers and pictures to so-called "safe zones", geofenced locations such as schools or home.

Apart from IT security and privacy issues, functions of these smart watches have been criticized for being either not functional and only simulating security, such as the SOS button, or potentially harmful to a child's development, like the tracking function [19].

2.3 Tablets for children

Tablets designed for children are a subcategory of educational toys aiming at children to provide entertainment as well as a learning component. While similar forms of electronic educational toys have been on the market for more than three decades, only recent technology made it possible to evolve from stand-alone computers to internet-connected tablets. Several tablets targeted at children run a regular version of Google's OS Android with a specially designed front end and customized apps

in order to serve children's needs. Researchers have shown with Vtech's Storio Max that—even though the special front end does not offer access to Android's interface—users can easily circumvent these settings. Moreover, Storio Max was proven to run on outdated software such as Android 4.2.2 and Linux Kernel 3.036, making it vulnerable to a number of security flaws [20]. Since Vtech fell victim to the above-mentioned hack in 2015, exposing millions of user data sets, children using educational tablets are also subject to this risk. With the nature of tablets using third party apps, the risk of collecting children's sensitive user data and storing it on servers around the world becomes even more prominent in tablets for children than in the aforementioned smart watches. This includes lack of control of the usage of this data by third parties [21].

2.4 Baby monitors

Baby monitors used to be simple radio systems to monitor infants in another room. Modern technology has widened possibilities including video surveillance, motion detection and two-way interaction, making modern baby monitoring similar to a regular CCTV system, and oftentimes security cameras are simply used as baby monitoring devices. As with many IoT products, these monitoring devices are often wirelessly connected to the internet and subject to attacks [22]. As with the products described above, these connected monitoring devices can bear the risks of unencrypted data transfer, insecure server infrastructure or weak and standard passwords [23]. While former baby monitors were accessible from the immediate vicinity, being connected to the internet and streaming their contents via a central server makes these products vulnerable to hacks. Since many of these devices offer mobile apps to monitor one's home while being away, just as with children's smart watches and connected toys, these apps can share information with several third-party providers.

3 Legal requirements

Legal requirements for the IT security of the products described above can result from special regulations for certain product groups on the one hand, but also from general regulations on the other. In the following, first the regulatory content of the EU Toy Safety Directive [24] is examined before general regulations, such as the Cybersecurity Act [25], the General Data Protection Regulation (GDPR) [26] and the Radio Equipment Directive (RED) [27], are dealt with. In addition to European law, German regulations are also analysed where relevant.

3.1 Toy Safety Directive

The Toy Safety Directive is the heart of European regulations for the safety of toys. In Germany it was transposed into national law by the Ordinance on the safety of toys (*Verordnung über die Sicherheit von Spielzeug*). The main content of the Toy Safety Directive is the obligation of manufacturers to guarantee certain characteristics of toys, as provided for in Art. 10. These can be physical and mechanical properties,

for example, but also non-flammability or chemical properties[1]. The Directive does not contain any regulations on IT security or a general clause on the security of toys. Furthermore, the Toy Safety Directive is only applicable if the IoT device in question is a toy within the definition in Art. 2 (1) of the Directive. According to this article, a toy is a product designed or intended, whether or not exclusively, for use in play by children under 14 years of age. In addition, Annex I No. 14 of the Directive clarifies that electronic equipment that is used to access interactive software and its associated peripherals is not a toy unless the electronic equipment or the associated peripherals are specifically designed for and targeted at children and have a play value of their own. Both exceptions limit the scope of the Toy Safety Directive to IoT devices but do not eliminate it completely. Manufacturers whose devices are to be classified as toys in accordance with Article 2 (1) must comply with the Toy Safety Directive. However, these requirements only concern the materials of the products. This could change in the context of the current ongoing evaluation of the Toy Safety Directive by the EU Commission [28]. Within the evaluation the consumer organisations ANEC—the European Consumer Voice in Standardisation (Feedback from: [29]) and BEUC—The European Consumer Organisation (Feedback from: [30]) have demanded the inclusion of specific regulations for the IT security of toys. A similar demand has also been made by the German Association of TÜV (VdTÜV). The Commission's adoption was originally planned for the second quarter of 2019 but has not yet taken place.

3.2 Cybersecurity Act

Besides objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA), according to Art. 1 (1) the Cybersecurity Act also contains a framework for the establishment of European cybersecurity certification for ICT products, ICT services and ICT processes. The Cybersecurity Act could be applicable to IoT devices if they represent ICT products. An ICT product is defined in Art. 2 (12) Cybersecurity Act as an element or a group of elements of a network or information system. IoT devices are part of a network and information system [31]. They are therefore ICT products. In addition to the devices themselves, which are usually owned by the end users, the IoT is also backed by a huge server infrastructure [31]. This is operated by the providers and is used for data evaluation but also for controlling the devices [31]. The latter is often done via an interface between the server system and an app or web interface managed by the user [31]. In these cases, the server system can be classified as a service consisting fully or mainly in the transmission, storing, retrieving or processing of information. It is then an ICT service as in Art. 2 (13) Cybersecurity Act. Recital 2 of the Cybersecurity Act, which explicitly focuses on the existing IT security problems in the IoT, also supports this classification. Devices for children, such as connected toys or child tablets, can also be classified as ICT products. If there is a server infrastructure behind the devices, it can be qualified as an ICT service. However, the Cybersecurity Act does not make any binding requirements for the IT security of IoT devices in

[1] See, Toy Safety Directive, Annex II.

general. Art. 46 et seq. of the Act provides only a voluntary certification framework. But there is no obligation for manufacturers to carry out certification. Against this background, it is questionable whether the Cybersecurity Act will lead to an improvement in the situation, particularly in the area of IoT devices.

3.3 General Data Protection Regulation

The GDPR is the core of the European data protection law and, according to Art. 2 (1), it is objectively applicable when personal data is processed wholly or partly by automated means. The territorial scope of application of the GDPR is broad and, according to Art. 3, covers not only processing within the EU but also outside, if goods or services are directed to data subjects in the EU. When IoT devices are used, large amounts of personal data of the user are usually processed by the provider. At the same time, these are usually either offers explicitly aimed at the European market or those provided by companies in the EU. In principle, the GDPR is therefore applicable to a large proportion of devices. However, there are exceptions if the device does not process personal data or if the exception in Art. 2 (2) a) GDPR applies. This is the case, for example, with the toy teddy bear "My friend Freddy" described above. The toy works via an app in which personal data of not only of the child but also of the family is stored. However, this data remains on the smartphone and is not transferred to the provider. The GDPR therefore does not apply to this toy and in similar cases.

If the GDPR is applicable—as in most cases—it requires the controller to take technical and organisational measures to protect personal data in accordance with Art. 32 (1) GDPR. Furthermore, Art. 25 (1) GDPR provides for the principle of data protection by design, which obliges the controller to consider technical and organisational measures to protect personal data as early on as during the development of the product. The requirements of the GDPR are formulated in a technologically neutral way and Art. 32 (1) GDPR mentions only some possible measures as examples. Nevertheless, the required security level is high and, if implemented correctly, could lead to a significant improvement in IT security on the IoT (an overview of the state-of-the-art of IoT security can be found at [32]).

In practice, however, since the introduction of the GDPR there has been no noticeable improvement in IT security in the area of IoT in general and in the area of IoT devices for children in particular. For example, the SonicWall Cyber Threat Report predicts that attacks on IoT devices will continue to grow in 2020 [33]. This disparity can be attributed in part to the heavy workload and inadequate resources of the data protection authorities. For example, the activity report of the "*Bayerisches Landesamt für Datenschutzaufsicht*" (Bavarian state data protection authority for the non-public sector) shows that the authority does not have sufficient resources to answer the large number of submissions [34]. In the case of IoT devices, enforcement of the GDPR is even more complicated, the reason being that measures according to the GDPR may only be directed against the controller. This means that measures of data protection authorities cannot be taken against manufacturers, suppliers, importers or sellers, even if the controller evades access by the authorities. In the case of IoT devices, controllers are often companies from East Asia. They often do not

have a branch in the EU and do not comply with their obligation under Art. 27 (1) GDPR to appoint a representative in the EU. Effective enforcement of the GDPR seems barely possible in these cases. The current legal situation thus rewards precisely those who observe the GDPR the least. Against this background, it is hardly surprising that many German companies perceive the GDPR as a competitive disadvantage [35]. This problem has also been recognised by the German data protection authorities and in their "*Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO*" (Report on the experience of the independent data protection supervisory authorities of the Federal Government and the states in applying the GDPR) they call not only for a development of data protection law in the direction of product liability, but also for an obligation to publish representatives in accordance with Art. 27 (1) GDPR, as is already the case for data protection officers in Art. 13 f. GDPR [36]. In conclusion, it can be stated that at the present time it is not to be expected that the GDPR will solve the massive problem of IoT security.

3.4 Radio Equipment Directive

According to Art. 1 (1) RED, the main purpose of the Radio Equipment Directive is to create a legal framework for the radio equipment market. With regard to ensuring IT security for IoT equipment, the Directive can be used to the extent that IoT equipment can be classified as radio equipment within the meaning of Art. 2 (1) No. 1 RED. Here, radio equipment is defined as an electrical or electronic product used for radio communication. If IoT devices communicate via radio links, such as Bluetooth or Wi-Fi, they meet the definition of Art. 2 (1) No. 1 RED and are therefore radio equipment within the meaning of RED [37]. A fundamental obligation to implement IT security measures is contained in Art. 3 (3) e) and f) RED. Accordingly, the equipment must be designed to ensure that the personal data and privacy of the user and of the subscriber are protected. They must also support features ensuring protection from fraud. However, the EU Commission has not yet defined any mandatory measures [38], which means that the manufacturer's obligation is currently in vain. Against the background of a public consultation of the Commission on Art. 3(3)(e) and (f) RED in November 2019 [39], the existing legal situation can be expected to be tightened. As a result, regulations could emerge that establish concrete safety requirements for radio equipment and thus for many IoT devices as well. The effectiveness of such a regulation, which is linked to the characteristics of a product rather than the processing of personal data, is shown, for example, by § 90 (1) sentence 1 TKG[2]. The law regulates the misuse of transmitting equipment and contains a ban on devices which can be misused for eavesdropping. Violations of this ban can be punished with up to two years in prison or with a fine

[2] § Section 90 (1) sentence 1 TKG can be translated as: It shall be prohibited to own, manufacture, market, import or otherwise bring in the area of application of this Act transmitting equipment or other telecommunications equipment which, by virtue of their form, simulate another object or which are covered with objects of everyday use and which, by reason of these circumstances or by virtue of their mode of operation, are particularly suitable and intended for listening to the non-publicly spoken word of another person unnoticed by the latter or for recording the image of another person unnoticed by the latter.

according to § 148 TKG. In addition, under § 115 (1) TKG, the Federal Network Agency can take appropriate measures to enforce compliance with the law by way of administrative proceedings. In this context, the Federal Network Agency may, for example, demand the destruction of prohibited equipment, but may also prohibit its sale or oblige dealers to disclose the buyers. Prohibited devices can be not only classic spy devices, such as hidden cameras in ashtrays or smoke detectors [40], but also IoT devices. For example, in addition to the doll "My friend Cayla" (see above), which was classified as illegal in 2017 [41], several of the children's smart watches mentioned above, which have a remote monitoring function, are also prohibited under § 90 TKG [40]. As a result of the ban, there is no longer a legal market for these devices in Germany. However, since § 90 TKG is primarily aimed at restricting the distribution of spy devices, the law in this form is not suitable for establishing IT security for all IoT devices.

4 Conclusion

Against the background of the security gaps described here, it can be seen that IT security for IoT devices for children is currently only insufficiently guaranteed. In this respect, these devices do not differ from other IoT devices despite their particularly vulnerable user group. The current situation is caused not least by a legal situation that on the one hand sets binding standards for only some of the devices and on the other hand is hardly enforceable, especially against those who disdain the applicable law the most. A solution to the situation, which is unsatisfactory both for companies that comply with the applicable law and for consumers, could be the implementation of product-related IT security standards by the EU Commission. Both the Toy Safety Directive and RED could soon have such rules in place.

Funding Open Access funding provided by project DEAL.

References

1. Juniper Research. Smart Toy revenues to grow by almost 200% from 2018 to $18 billion by 2023. https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-grow-almost-200pc-by-2023. Accessed 16 Sep 2020
2. Tsukayama. Mattel has canceled plans for a kid-focused AI device that drew privacy concerns. https://www.washingtonpost.com/news/the-switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it/. Accessed 16 Sep 2020
3. Forbrukerradet. #Toyfail: An analysis of consumer and privacy issues in three internet-connected toys. https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf. Accessed 16 Sep 2020

4. Nordrum. Popular Internet of things forecast of 50 billion devices by 2020 is outdated. https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated. Accessed 16 Sep 2020
5. International Working Group on Data Protection in Telecommunications. Privacy risks with smart devices for children. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2019/2019-IWGDPT-Working_Paper_Smart_Devices.pdf. Accessed 16 Sep 2020 (Working paper)
6. Charta of Fundamental Rights of the european Union. Article 24.
7. Dellinger. Survey says Siri and Google assistant are the most used voice assistants. https://www.digitaltrends.com/home/siri-google-asistant-most-used-voice-assistants-alexa/. Accessed 16 Sep 2020
8. FAQ about cyber attack on Vtech learning lodge. https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge. Accessed 16 Sep 2020
9. Forbrukerradet. Connected toys violate European consumer law. https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/. Accessed 16 Sep 2020
10. Hessel. "My friend Cayla" – eine nach § 90 TKG verbotene Sendeanlage?. JurPC (13). https://www.jurpc.de/jurpc/show?id=20170013. Accessed 16 Sep 2020
11. Bundesnetzagentur. Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html. Accessed 16 Sep 2020
12. BEUC. Cayla's secret food tips. http://www.beuc.eu/food-marketing-children-game-over-0#caylassecretfoodtips. Accessed 16 Sep 2020
13. Pen Test Partners. Making children's toys swear. https://www.pentestpartners.com/security-blog/making-childrens-toys-swear/. Accessed 16 Sep 2020
14. Daniel. How children's smart watches may contain hidden security flaws. https://www.verdict.co.uk/childrens-smart-watches/. Accessed 16 Sep 2020
15. Forbrukerradet. #WatchOut: Analysis of smartwatches for children. https://fil.forbrukerradet.no/wp-content/uploads/2018/03/watchout-rapport-october-2017.pdf. Accessed 16 Sep 2020
16. EU-Commission. The rapid alert system for non-food products (RAPEX). Alert number: a12/0157/19. https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en. Accessed 16 Sep 2020
17. Forbrukerradet. #WatchOut: Analysis of smartwatches for children. https://fil.forbrukerradet.no/wp-content/uploads/2018/03/watchout-rapport-october-2017.pdf. Accessed 16 Sep 2020
18. Judd. Smartwatch apps let parents keep track of their kids but data breaches mean strangers can watch them too. https://mobile.abc.net.au/news/2020-02-11/gps-tracking-watch-security-bug-data-breach-personal-info/11909478. Accessed 16 Sep 2020
19. Forbrukerradet. #WatchOut: Analysis of smartwatches for children. https://fil.forbrukerradet.no/wp-content/uploads/2018/03/watchout-rapport-october-2017.pdf. Accessed 16 Sep 2020
20. VTech Storio Max Vulnerability - CVE-2018-16618. https://www.surecloud.com/services/blog/vtech. Accessed 16 Sep 2020
21. International Working Group on Data Protection in Telecommunications. Privacy risks with smart devices for children. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2019/2019-IWGDPT-Working_Paper_Smart_Devices.pdf. Accessed 16 Sep 2020 (Working Paper)
22. Wang. I am in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say. https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/. Accessed 16 Sep 2020
23. Wie Sie eine Baby-Cam erfolgreich hacken. https://sec-consult.com/blog/2018/06/wie-sie-eine-babycam-erfolgreich-hacken/. Accessed 16 Sep 2020
24. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys.
25. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
26. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
27. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

28. EU Commission. Evaluation of the toy safety directive. https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-3667279_en. Accessed 16 Sep 2020
29. ANEC, the European consumer voice in standardisation. https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-3667279/feedback/F13698_en?p_id=262846. Accessed 16 Sep 2020
30. BEUC—The European Consumer Organisation. https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-3667279/feedback/F13693_en?p_id=262846. Accessed 16 Sep 2020
31. Silva, Rodrigues, Saleem, Kozlov, Rabelo (2019) M4DN.IoT—A networks and devices management platform for Internet of things. IEEE Access, vol. 7, pp 53305–53313, 2019, https://doi.org/10.1109/ACCESS.2019.2909436
32. NISTIR 8259 (Draft) (2020) Recommendations for IoT device manufacturers: foundational activities and core device cybersecurity capability baseline. https://doi.org/10.6028/NIST.IR.8259-draft2. Accessed 16 Sep 2020
33. Sonicwall. Cyber threat report 2020. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/. Accessed 16 Sep 2020
34. Bayerisches Landesamt für Datenschutzaufsicht. 9. Tätigkeitsbericht, 2019. https://www.zaftda.de/tb-bundeslaender/bayern/aufsichtsbehoerde-1/718-9-tb-noeb-bayern-2019-keine-landtagsdrucksache-28-01-2020/file. Accessed 16 Sep 2020 (S. 10 ff. (German))
35. Engels, Scheufen. Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung, IW-Report 1/20. https://www.iwkoeln.de/fileadmin/user_upload/Studien/Report/PDF/2020/IW-Report_2020_DSGVO_und_Wettbewerb.pdf. Accessed 16 Sep 2020 (German)
36. Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO. https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf. Accessed 16 Sep 2020 (German)
37. EU Commission. Guide to the radio equipment directive 2014/53/EU, version of 19 december 2018. https://ec.europa.eu/docsroom/documents/29782. Accessed 16 Sep 2020 (p. 10 f.)
38. EU Commission. Guide to the radio equipment directive 2014/53/EU, version of 19 december 2018. https://ec.europa.eu/docsroom/documents/29782. Accessed 16 Sep 2020 (p. 37)
39. EU Commission. Radio Equipment Directive (RED). https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en. Accessed 16 Sep 2020
40. Bundesnetzagentur. Hinweise zu einzelnen Produktkategorien. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/MissbrauchSendeanlagen/HinweiseProduktkategorien/hinweiseproduktkategorien.html. Accessed 16 Sep 2020 (German)
41. BBC. German parents told to destroy Cayla dolls over hacking fears. https://www.bbc.com/news/world-europe-39002142. Accessed 16 Sep 2020