Dynamic Consent: Physical Switches and Feedback to Adjust Consent to IoT Data Collection

Henrich C. Pöhls[1(✉)] and Noëlle Rakotondravony[2]

[1] Institute of IT-Security and Security Law, University of Passau, Passau, Germany
hp@sec.uni-passau.de
[2] Worcester Polytechnic Institute, Worcester, MA, USA
ntrakotondravony@wpi.edu

Abstract. From smart homes to highly energy-optimized office building and smart city, the adoption of living in smart spaces requires that the inhabitants feel comfortable with the level of data being collected about them in order to provide smartness. However, you usually provide this consent on—or best before—your very first interaction. Thus, firstly your consent might vary over the time of usage. Secondly, it is not always obvious if data is currently collected or not. This paper addresses two missing elements in the interaction with a smart environment: First, the general concept of dynamicity of consent to data collection. Second, provision of a physical interaction to gather and change consent and a physical feedback on the current data collection status. By the feedback being physical we mean being visual, haptic or accoustic, in order to allow natural perception by the users in the physical space. For both components we provide examples which show how one could make both the current status as well as the consent physical and discuss the user perception. We argue that having a physical interaction to start potentially privacy-invasive data collections is a useful enrichment for legal consent, and physically visible status is helpful to make a decision.

Keywords: Privacy · Security · Consent · Smart living · Internet-of-Things

1 Introduction and Motivation

We need privacy in the smart spaces that are enabled by the technological advances of the Internet-of-Things (IoT). Privacy can be seen as a legal right, like the European Union's General Data Protection Regulation (GDPR) [1], or even as a human right [2]. Regardless how you see it, it might get demanded by your users as their fundamental criteria for adopting smart spaces, and thus the invasiveness of smart objects must be limited and users' control on data collection must be enabled.

Henrich C. Pöhls—Supported by EU H2020 grant n°780315 (SEMIoTICS).

N. Streitz and S. Konomi (Eds.): HCII 2020, LNCS 12203, pp. 322–335, 2020.
https://doi.org/10.1007/978-3-030-50344-4_23

Data protection laws, like the mentioned GDPR in the EU, require—among other things—to "minimise the amount of collected data" [3] and that the data subject, which is the individual person whose personal data is handled, needs to give their informed consent a-priori to the data gathering process and must be able to intervene. There are different technical mechanisms to achieve the recommendation that "Device manufacturers should limit as much as possible the amount of data leaving devices" [3]. For instance, reasearch findings from the EU-funded project RERUM (2016)[1] sparked works that allow for more configurable privacy and data minimisation of private information such as location) [4–6]. And clearly, the need for privacy(-by-design) is acknowledged not only within the EU [7], but also elsewhere, e.g. Canada [8].

Following the EU's GDPR the data subject has the right to intervene or update/revoke their consent. M. Weiser's vision of ubiquitous computing [9] partly become reality, with smart things that monitor us directly or indirectly in our physical surrounding: in our smart homes [10], in the smart city with smart street lamps[2], and smart buildings[3].

Allhoff et al. [11] also outlined that even if the monitored inhabitant of a such a smart space, i.e. the legal data subject, would have been informed of the personal information being collected and would have given consent, there will still be occasions were they would not want to leave the usual traces in the smart space, e.g. during private celebrations. However, after having initially consented to the collection there would still be occasions were one would like to object and avoid to leave the usual traces in the smart space, e.g. if you hide easter eggs, secretly prepare birthday cakes, have surprise parties or play Papa Noël.[4]

Furthermore, as we are at the level of physical interaction with smart spaces, we propose that the human-computer-interaction interface for those dynamic adaption of consent should also be a physical one. We would like to extend the statement that "Truly smart gadgets should have built-in intelligence"[5] [12], such that the users of those smart gadgets shall be enabled to easily adjust the data collection dynamically to provide them "[...] the ability to perceive and control who is observing or disturbing a user in her private territory [...]" [13]. In this work we introduce first the general requirement for dynamicity in consent and then discuss physical-interaction based human-computer-interaction (HCI) concepts—physical both in the signalling of the inhabitants' wish of consent and in the signalling of the smart devices' or smart spaces' current collection activity. In the following, we first discuss our first contribution of the notion of dynamicity in Sect. 2 and then discuss existing related works that allow physical interaction with the privacy settings within the SmartHome use-case Sect. 3, before we conclude in Sect. 4.

[1] `ict-rerum.eu` (accessed 30 Nov 2019).
[2] https://www.tvilight.com (accessed 30 Nov 2019).
[3] https://www.greenerbuildings.eu (accessed 30 Nov. 2019).
[4] These examples emerged from several open discussions with users of IoT enabled spaces we conducted in preparation of this work.
[5] Proclaimed by Tony Fadell, the inventor of Nest thermostats.

2 New Concepts: Dynamicity of Consent and Physical Interaction Patterns

In this work we introduce two new concepts: dynamicity of consent and physical interaction patterns. The terminology are briefly distinguished and defined in this section.

2.1 Definition: Dynamicity of Consent for Data Collection in the Physical Space

We would define the general concept of changing consent for data collection in a physical surrounding, in contrast to the virtual world, e.g. when browsing the WWW, in a dynamic manner as follows:

> *Dynamicity of consent allows the user who is subject to data collection in the physical space the user interacts with to adapt their consent to a defined set of rules for data collection.*

In EU GDPR [1] terms the user is known as the 'data subject' and thus dynamic consent enables data subjects to change their informed consent dynamically from (partial or full) opt-in to (partial or full) opt-out or vice-versa. In the following we will use the term context, there are two contexts in our environment: the context of the physical world, with buttons and sensors and actuators; and the virtual context, requiring the use of additional devices for the interaction, like smart phones, tablets, computers, touch screens. In this respect the notion of a context switch would mean that the user is required to change between the contexts to fulfil a task, e.g. a switch from physical to virtual interfaces would be to take out the smartphone, open an app to dim the light. From the perspective of the user the following requirements shall be fulfilled:

- *change of consent requires no context switch*
- *checking current status requires no context switch*
- *the currently signalled status is correctly representing the data collection*

The final point requires that the system is designed and deployed such that a certain data collection would not be carried out if the visual suggests to the user that it is not taking place, i.e. no malicious application can circumvent the indication of the current status [14].

2.2 Definition: Physical Switch

> *A physical switch allows the user, who is subject to data collection in the physical space that the user interacts with, to change their consent to a different defined set of rules for data collection by a physical interaction.*

In this context it is important to note, that our current work sees voice commands not as a physical interaction. This has several advantages, firstly an attacker

could not carry out the change and maliciously re-enable previously disabled data collections from a distance, e.g. not like the laser attack on voice-enabled which allows to inject commands over long-distances of line of sight [15] or by maliciously playing non-hearable commands [16,17]. Secondly, it allows to use the physical gesture or interaction as a stronger signal signalling informed consent.

2.3 Definition: Physical Kill Switch

A physical kill switch allows the user, who is subject to data collection in the physical space that the user interacts with, to physically either completely disable the data collection or reduce it to a defined lower level by a physical interaction.

This is slightly different to the physical switch, that would not require the data collection opt-out to be physically enforced or at least physically diminished. An obvious example for a kill switch is to take the battery out of a device or put a covering lid over a camera.

2.4 Kill Switch Compared Normal Switch

Both, the physical kill switch as well as the physical switch, can be used to opt-in or opt-out of data collection. For a discussion of opt-in or opt-out and problems the reader shall turn to other works, e.g. [8,18,19]. We note no effect with respect to the general opt-in vs. opt-out discussion whether or not the switch is physical or virtual. Thus, both switches suffer from the generic problem of how they should be initially configured.

The subtle difference is that the physical *kill* switch is defined to physically diminish or remove the device's ability to collect the data in question. This means that when a *normal* switch is turned to the 'off' position the device could still technically gather the data and signal the back-end to not safe or process the data further, i.e. it can still physically collect the data. The beauty of having a user physically interact with the device allows to use the physical switch to also physically disable (or diminish) the device's ability, i.e. the power supply is physically disconnected, or the sensor physically blocked.

Note that the information of the current consent, i.e. if the user allows data being currently collected or not, is not part of the information that the physical switch is trying to disable.

Finally, whether or not this physical blockage is easy to understand or note for the average user is not part of the differentiation. If it is easy to note for the user, the physical kill switch often also doubles as a physical indicator, which we define next.

2.5 Definition: Physical Status Indicator

A physical status indicator allows the user to physically perceive the current state of the data collection it is subject to while acting within this space.

Note, this makes two important underlying assumption: Firstly, the user understands what level of data collection means what level of privacy-invasiveness, which requires that the user needs to be previously informed about the consent. Secondly, the status indicated must not be circumvented maliciously [14].

3 Use-Case and Examples

Taking the terminology previously sated, we are briefly describing and discussing different physical kill switches and physical status indicators of data collections; we do not strictly limit ourselves to those in IoT or smart home scenarios when it comes to widely used existing ones.

3.1 Physical Kill Switches

Many physical kill switches found in existing products offer a physical gesture and result in two or more visually different positions of the switch, thus they immediately can serve as physical status indicators as described in Subsection 3.3. Examples of kill switches are physical switches which require physical interaction to opt-out or opt-in into data collection, but instead of programmatic switching the status of data collection they physically diminish the ability to collect certain data. However, as a physical switch usually has different states, e. g., on- and off-state, they can also serve as physical indicators for the state they control. Different in their physical feedback to switches are push buttons, as they do not have a state; so even though they are physical they offer no indication of their position by themselves; but they require a physical interaction with the human user.

In general, the same discussion on opt-in being better than opt-out for privacy is the same in the physical world as in virtual worlds and has been discussed there, e. g., for cookies and tracking in websites.

As an example take the Amazon Echo depicted in Fig. 1. The device has "[...] a microphone off button that electronically disconnects the microphones"[6]. The device features a physical push button, for which the device manufacturer claims it controls the power supplied to the audio collection circuit and thus physically disables the all device's microphones. It also turns an LED-illuminated ring to the color red. The state survives reboots, but the transparency, i.e., the understandability, of the physical disablement of the data collection is not as obvious as a physical lid that covers a camera (Fig. 4, 5), or a physically disconnected sensor (Fig. 3). To make sure that it is not maliciously tampered with might require skilled third-parties to confirm the physical kill by testing a device sample (e.g. someone who dissects such hardware to see if it truly disables the power[7]).

[6] https://www.amazon.com/Alexa-Privacy-Hub (accessed Nov. 2019).
[7] Compare the attacks to bypass the indicator of a webcam [14].

Fig. 1. Amazon's button to turn off the microphone and the red-illuminated ring as an indicator [www.amazon.com/Alexa-Privacy-Hub] (Color figure online)

3.2 Physical Status Indicators

Regardless of the way data collection is controlled, there is the possibility to offer feedback in the physical world about the current status of the data collection. Probably the most common example of such an indicator is a visual indication by turning on a light emitting diode (LED). This can be found on many devices, e.g. on voice-controlled products the "[...] button turns red [when] the microphone is off. The device won't respond to the wake word or the action button until you turn the microphone on again."[8]. Additionally, other visual feedback can be provided, e.g. as depicted in Fig. 1 the red-illuminated ring also signals that microphones and thus voice data collection is turned off. On the contrary, when data is being collected "[...] a blue light indicator will appear or an audio tone will sound [...]"[9].

Another example of a physical status indicator is the LED next to many webcams, that shall light-up while the device is capturing images. This is a visual that is well understood by human users and allows to identify when live images are captured, however it usually does not flash when still images are taken.

A note on the security requirements on status indicators: Special care needs to be taken to make sure the status indicator would stay in-sync with the data acquisition, e.g. Apple build their hardware such that usually software would not be able to turn on the live-imaging without turning on the light, i.e. the visual indicator is paired in hardware. "Since the LED is controlled by the same output that controls STANDBY [meaning the camera is not capturing], there is no danger that firmware on the EZ-USB could deassert STANDBY and turn the LED off [...]" [14]. We say 'usually' because researchers were able to modify the hardware's programming (firmware) to enable the capturing while still signalling that the camera is in "STANDBY" and thus "[...] control the LED without affecting the operation of the image sensor." [14]. However, it is out of scope to discuss the security of the status indicator operation in this paper.

[8] https://www.amazon.com/Alexa-Privacy-Hub (accessed Nov. 2019).
[9] https://www.amazon.com/Alexa-Privacy-Hub (accessed Nov. 2019).

Noteworthy, for the physical status indicators—the same for software ones—it is a requirement that the indicator is always truly reflecting the current state of the data collection.

Fig. 2. External disconnect-able microphone serves as both (a) physical kill switch and (b) indicator; taken from the Candle IoT project [www.candlesmarthome.com]

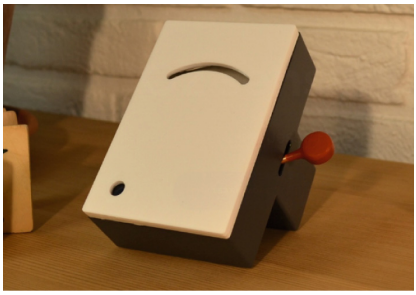

Fig. 3. Big red handle serves as both (a) physical switch and (b) indicator for the Candle IoT project's carbon sensor [www.candlesmarthome.com] (Color figure online)

3.3 Mixes of Switch and Status Indicators

As mentioned earlier, a lot of examples offer physical kill switches serve a double role and also function as physical status indicators. For example, the switch in Fig. 3 also serves as an indicator. Following the designer's statement the "big red toggle will automatically move to the correct position to indicate it's no longer sending data. This allows you to always figure out if the device is currently transmitting data, even when looking at it from across the room."[10]. Other switches might provide more subtle status indicators, e.g. the camera being covered and some orange-red-coloured plastic appears as depicted in Fig. 4 and 5. Another way of switching on or off data collection is to disconnect the sensors relevant for data collection physically, as depicted in Fig. 2. Except for the first one, depicted in Fig. 3, the physical kill switches also physically hinder the data collection, i.e. covering or disconnecting the sensor. We thus introduced a distinction of the physical kill switch from the physical switch as discussed in Sect. 2.

A completely different form of physical interaction was for example executed during a security and privacy related conference (S&P conference in May 2019): They distributed black stickers that participants had to stick on their badges if they did not want to be filmed. This is again an opt-out, and signals privacy non-consent in the physical world. Technically, it would be possible to create recognisable visuals that people put on visible areas on their body for cameras

[10] https://www.candlesmarthome.com/jesse-howard-innovations (accessed Dec. 2019).

Fig. 4. Physically closable lid, denoted '6. Integrated privacy shade', serves as both (a) physical kill switch and (b) indicator for Logitech's webcam from 2009 [download01.logitech.com/24391.1.0.pdf]

Fig. 5. Physically closable lid acts as both (a) physical kill switch and (b) indicator for the camera build in the Amazon Echo Show 5 [www.amazon.com/Alexa-Privacy-Hub]

to pick-up and recognise to then consequently blur their faces locally before forwarding their images. As a side note, of course this shall not be confused and lead to the discussion if criminals would abuse those stickers to blur their images on security cameras. This is not acceptable, but areas that require constant video monitoring for security should also be limited. To conclude this side discussion, this work's scope is on the ability of legally opting out of data collection dynamically due to changes in the privacy-invasiveness tolerate-able by users due to changes in their situations.

Another example is the updates Amazon made to their devices of the models including a camera, named Echo Show: Compared to earlier models they added a "[...] built-in shutter [that] also lets you easily cover the camera." as depicted on their website and reproduced as Fig. 5. Noteworthy to say, Amazon is not the first to produce this hardware kill switch for their camera-including products, many notebook vendors, amongst them market leaders Lenovo[11], HP[12]; also some early external USB webcams already had the physical lid on them, e.g. the 1.3 MP Webcam C500 V-U0006 from 2009 featuring an "integrated privacy shade" (see Fig. 4). Note that this switch was not continued throughout all models of

[11] See for example Lenovo's Blog Post from 2010 on the ThinkCentre M90z http://blog.lenovo.com/en/blog/watch-that-webcam (accessed Jan. 2020).

[12] See for example the top-listed feature of "a physical shutter to protect from malicious surveillance." https://www8.hp.com/uk/en/solutions/computer-security.html (accessed Jan. 2020).

Logitech[13]. Today there is a plethora of webcam covers as physical add-ons for camera-including products, from sticky tape, as used quite famously by Mark Zuckerberg [20], to stickers of pro-privacy NGOs[14], to 3D-printed covers for certain webcam models[15].

3.4 Overview of Possibilities to Signal and Change the Status of Consent to Data Collection

Table 1 gives an overview how the discussed possibilities of physical switches and physical indicators for feedback can be combined and the level of dynamic consent control that can be exercised by them.

Table 1. Combination of switch and indicator for control of dynamic consent (higher level means better control; above level 2 is recommended)

Switch \ Indicator	Visual	Haptical/Audio	No Indicator
Physical Switch	Level 3	Level 2	Level 1
Physical Kill Switch	Level 5	Level 4	Level 1
No Switch	Level 1	Level 1	Level 0

We have categorized the control that can be exercised into four ascending levels, starting from level 0 that allows no easy physical control of the data collection activities. We suggest any smart environment to achieve at least level 2 for an interactive physical consent management, thus we have marked those as grey in Table 1. The following descriptions, especially the examples, of the levels are written explicitly in non-technical language to allow them to be used to ask participants in a more formal user study. In all levels we assume that the user did give informed consent to data collection before the first interaction, i.e. during initial setup.

Level 0: In the physical environment the user does not know if data is currently being collected and he can not change the current data collection. The user can only go to a website or interact with an app on its mobile to see the current status and change the current data collection.
Example 0: User does not know if the smart home currently collects any data and can not change that without opening an app on the smartphone.

[13] For example there are third-party vendors selling physical covers, like for the Logitech C920 Webcam https://www.youtube.com/watch?v=2uNMcJXt0fo (accessed Jan. 2020).
[14] https://supporters.eff.org/shop/eff-sticker-pack (accessed Dec. 2019).
[15] https://www.thingiverse.com/thing:2003903 (accessed Dec. 2019).

Level 1: In the physical environment the user either does not know if data is currently being collected or the user can not change the current data collection from within the physical environment. The user still has to go to a website or interact with an app on its mobile to either see the current status of the data collection or change the current data collection.
Example 1a (no indicator, but switch): User can flip a physical switch, but then has to go to an app on the smartphone to see if its really changed the data collection.
Example 1b (no switch, but indicator): User can see a physical indicator, e.g. a red blinking LED, but then has to go to the app on the smartphone to turn off the data collection.

Level 2: In the physical environment the user is able to change the current data collection and on change is provided with a haptical or acoustical feedback. The user either has to interact with the switch again to receive feedback of the current data collection or go to a website or interact with an app on its mobile to see the current status of data collection.
Example 2a (vibration after toggling switch): User can flip a physical switch, which then vibrates twice if data collection is turned off or once if its turned on.
Example 2b: (spoken announcement after pressing a physical button): User can press a physical button, which then results in an audible announcement like 'collection off' if data collection is turned off or 'collection on' if collection is turned from off to on.

Level 3: In the physical environment the user is able to change the current data collection by a physical interaction and on change the user is visually provided with the current status. Thus the user does neither need to physically interact with the switch again to receive feedback of the current data collection, nor does need to switch to a website or an app.
Example 3 (LED changes color after pressing a physical button): User can press a physical button, which then results in an LED to glow in green color if data collection is turned off or glow in red color if collection is turned on.

Level 4: In the physical environment the user is able to change the current data collection and on change is provided with a haptical or acoustical feedback. The user either has to interact with the switch again to receive feedback of the current data collection or go to a website or interact with an app on its mobile to see the current status of the data collection. Additionally, the user's action physically intervenes with the sensor's ability for collecting the data[16].
Example 4: (spoken announcement after pressing a physical button): User can press a physical button, which then results in an speaker giving a spoken announcement like 'collection off' if data collection is physically disabled and thus turned off or 'collection on' if collection is turned on.

Level 5: In the physical environment the user is able to physically interrupt the current data collection by a physical interaction and the user can review the

[16] We note here, that of course the fact that data is not being collected is information that can still be collected.

current status easily by visual inspection. Thus the user does neither need to physically interact with the kill switch again to receive feedback of the current data collection, nor does need to switch to a website or an app. Additionally, the user's action physically intervenes with the sensor's ability for collecting the data[17].
Example 5 (visual indicator plus a physical kill switch): User can remove the sensor's cable, which physically disconnects the power to the sensor, which results in the sensor to stop glowing white and stop working which means that the collection is turned off; plugging it in will result in it starting to glow white and to collect data again.[18]

Table 2 shows which level the previously discussed real-life examples from Sect. 3 achieve. This table and the collected examples are by no means complete, finding real-life examples for the other levels is left for further research.

Table 2. Levels of physical control over dynamic consent reached real-world examples

Switch \ Indicator	Visual	Haptical/Audio	No Indicator
Physical Switch	**Level 3:** Big-handed switch (Fig. 3)	Level 2: -	Level 1: –
Physical Kill Switch	**Level 5:** disconnect-able microphone (Fig. 2); lid over webcam (Fig. 4,5); red LED on powerless, thus muted microphones (Fig. 1)	Level 4: –	Level 1: –
No Switch	**Level 1:** LED next to laptop webcam	Level 1: –	Level 0: –

3.5 Initial User Pre-study

We did conduct a very initial pre-study by open discussions with selected user groups. This was conducted to initially understand if users would value the concept of dynamic consent. We fully disclose all the details in this subsection. We did interview two groups: The first group consisting of five computer science students that are technically savvy and privacy-aware and a group consisting of eight normal users that were explained the ideas of living in a smart home

[17] We note here, that of course the fact that data is not being collected is information that can still be collected.

[18] We are aware that a non-glowing sensor would not enable the user to distinguish from a malicious or faulty sensor that is plugged-in and collecting data but not glowing; however we wanted to convey to users an example that physically disconnects the data gathering device.

environment. Both were presented the concept of dynamic consent and the idea of having physical switches to control the data collection of devices, e.g. presence monitoring and behavioural monitoring, using some of the real-world examples as given in this paper. Note, that the second group was not chosen totally distinct, it included older people and people exposed to new technology as users only, i.e. parents and friends of the computer science students from the first group.

As expected the first group explained that one might want to technically control the devices' ability to communicate with external servers, e.g. "flash open source firmware", "run your own MQTT-server locally", and "give suspicious devices no Internet by using a firewall rule" where among the answers. None of the participants found the concept of physical interaction bad in principle, some stated that they might not need it as they "already put tape over the laptop's webcam", or raised concerns that they might be "too lazy to get up to turn certain device functions physically off and thus leave it always on".

The second group—the group of normal users—seemed mostly reluctant to put technical 'gadgets' into their homes themselves and made statements, like "I do not want my home to always spy on me", which indicated to us that they have to be considered as privacy-aware as well. After being explained the concept of dynamic consent and physical interactions to control the consent, the members of the second group liked the idea, mainly making statements indicated that this allows them being "in control of all that technical stuff". During the discussion members of the second group also came up with more concrete usage scenarios: "having a switch near the front door which turns all monitoring on only when I want it".

As mentioned, due to the setup and the open discussions we had with them, the results can not be considered a user study, but we wanted to share the initial feedback we gathered. More structured interviews with focus groups especially including not-yet privacy-aware users would be beneficial for further research.

4 Conclusion

Clear and informed consent from the legal data subject is essential for smart spaces in order to comply to legal requirements and for human users in order to wisely adopt privacy-invasive technologies [21]. While in general, most users provide their consent to data collection mechanisms during initial device configuration, only few are aware of available interaction mechanisms with their smart surroundings for adjusting already accepted data collection terms.

We describe the concept of physically giving consent and also signalling the current state of data collection through visual, haptical, or audio feedback. This enables to interact easily and enables dynamically adaptable consent to data collection; a concept which we introduced in this paper as well. The concept describes how to leverage state-of-the-art devices' physical interfaces to dynamically empower users to dynamically adapt their consent to change from an already defined level of consent to data collection to another one. This means the user can make a physical interaction with the user's physical surroundings to

control the data collection the smart devices in the user's physical surroundings are gathering.

This way the user regains some control over the privacy invasion by smart things, as Könings et al. put it "The goal of territorial privacy is to control all physical or virtual entities which are present in the user's virtual extended territory in order to mitigate undesired observations and disturbances, and to exclude undesired entities from the private territory." [22]. Especially, the physical interaction with consent controls requires no change of context, i.e. the user does not have to use an app on the smart phone—switch to the virtual context—to dynamically change the consent to a physical spaces's data collection.

Further research is needed to show which other physical switches and feedback mechanisms are possible and what combinations thereof, and how users conceive more precise implementations of the concept.

Acknowledgment. H. C. Pöhls was partially funded by the European Union's H2020 grant n^{o}780315 (SEMIoTICS). This paper reflects only the authors' views.

References

1. European Parliament and the Council of the European Union: 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). Off. J. **OJ L**, 1–88, May 2016. 119 of 4.5.2016
2. OECD: The OECD Privacy Framework (2013). http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed Jan 2020
3. EU Article 29 Data Protection Working Party (WP 223): Opinion 8/2014 on the Recent Developments on the Internet of Things, pp. 1–24, September 2014
4. Pöhls, H.C., et al.: RERUM: building a reliable IoT upon privacy- and security-enabled smart objects. In: Wireless Communications and Networking Conference Workshop on IoT Communications and Technologies (WCNC 2014), April 2014, pp. 122–127. IEEE (2014)
5. Tragos, E.Z., et al.: Enabling reliable and secure IoT-based smart city applications. In: Proceedings of the International Conference on Pervasive Computing and Communication Workshops (PERCOM 2014), March 2014, pp. 111–116. IEEE (2014)
6. Staudemeyer, R.C., Pöhls, H.C., Watson, B.W.: Security and privacy for the Internet of Things communication in the SmartCity. In: Angelakis, V., Tragos, E., Pöhls, H.C., Kapovits, A., Bassi, A. (eds.) Designing, Developing, and Facilitating Smart Cities, pp. 109–137. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-44924-1_7
7. Danezis, G., et al.: Privacy and data protection by design - from policy to engineering. Tech. rep. European Union Agency for Network and Information Security, December 2014
8. Cavoukian, A.: Privacy by design: the 7 foundational principles. Revised Version. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf. Accessed Nov 2019
9. Weiser, M.: Some computer science issues in ubiquitous computing. Commun. ACM **36**(7), 75–84 (1993)

10. Frizell, S.: This Startup is Trying to Create - and Control - the Internet of Your Home. Time Mag. **184**(1) (2014). https://time.com/magazine/us/2926387/july-7th-2014-vol-184-no-1-u-s/
11. Allhoff, F., Henschke, A.: The Internet of Things: foundational ethical issues. Internet of Things **1**, 55–66 (2018)
12. Vella, M.: Nest CEO Tony Fadell on the future of the smart home. Time Mag. **184**(1) (2014). https://time.com/magazine/us/2926387/july-7th-2014-vol-184-no-1-u-s/
13. Könings, B., Schaub, F.: Territorial privacy in ubiquitous computing. In: 8th International Conference on Wireless On-Demand Network Systems and Services, pp. 104–108. IEEE (2011)
14. Brocker, M., Checkoway, S.: iSeeYou: disabling the MacBook webcam indicator LED. In: 23rd USENIX Security Symposium (USENIX Security 14), pp. 337–352 (2014)
15. Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D., Fu, K.: Light commands: laser-based audio injection on voice-controllable systems (2019). https://lightcommands.com/. Accessed 13 Dec 2019
16. Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., Xu, W.: Dolphinattack: inaudible voice commands. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 103–117. ACM (2017)
17. Roy, N., Shen, S., Hassanieh, H., Choudhury, R.R.: Inaudible voice commands: the long-range attack and defense. In: 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), pp. 547–560 (2018)
18. Karegar, F., Gerber, N., Volkamer, M., Fischer-Hübner, S.: Helping john to make informed decisions on using social login. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, SAC 2018, New York, NY, USA, pp. 1165–1174. Association for Computing Machinery (2018). https://doi.org/10.1145/3167132.3167259
19. Johnson, E.J., Bellman, S., Lohse, G.L.: Defaults, framing and privacy: why opting in-opting out. Mark. Lett. **13**, 5–15 (2002)
20. The Guardian - Alex Hern: Mark Zuckerberg tapes over his webcam. Should you?, June 2016. https://www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook. Accessed Dec 2019
21. Rosner, G., Kenneally, E.: Clearly opaque: privacy risks of the Internet of Things. In: Rosner, G., Erin, K. (eds.) Clearly Opaque: Privacy Risks of the Internet of Things, 1 May 2018. IoT Privacy Forum (2018)
22. Könings, B., Schaub, F., Weber, M.: Privacy and trust in ambient intelligent environments. In: Ultes, S., Nothdurft, F., Heinroth, T., Minker, W. (eds.) Next Generation Intelligent Environments, pp. 133–164. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-23452-6_4