

ConnectivityControl: Providing Smart Home Users with Real Privacy Configuration Options

Sebastian S. Feger, Maximiliane Windl, Jesse Grootjen, and Albrecht Schmidt

LMU Munich, Munich, Germany

Abstract. Smart home devices become increasingly popular as they allow to automate tedious tasks and often provide a wide variety of entertainment features. Yet, this increase in comfort comes at the cost of exposure to privacy risks as connected devices in smart homes capture most sensitive user data, including video, audio, and movement data of the inhabitants and guests. Smart home owners and bystanders typically have very limited control over these recordings. While few devices do provide physical artifacts to block individual sensors, deactivating recording and transmission capabilities typically requires powering devices off or disconnecting them from the network, typically rendering these smart home appliances useless. In response, we created *ConnectivityControl*, a framework that allows users to switch between four device connectivity levels: Offline, Access Point mode, Local Network mode, and Online. *ConnectivityControl* features a privacy label that depicts how those modes impact device features and privacy exposure. The label can be used to inform purchase decisions and to monitor devices across their lifetime. In this paper, we detail the system architecture and the interaction design and showcase *ConnectivityControl*'s implementation in the context of two common smart home systems: a smart camera and an environmental sensing unit. Finally, we discuss how *ConnectivityControl* and its labels can transform the way smart home users configure their systems to match individual privacy needs.

Keywords: Privacy label · ConnectivityControl · ConnectivityLabel · Effective smart home privacy configuration.

1 Introduction and Related Work

The number of installed smart home devices has been growing rapidly in recent years. These devices provide comfort by automating tasks and creating supportive environments. They are also fitted with an increasing number of sensors and actuators to further benefit their users. The evolution of smart speakers makes for a good example: initially focused on microphones and speakers, some modern versions additionally come with cameras, displays, and even motors to adapt to users moving in their homes. While any additional sensor and actuator promises an increase in the number of features and the level of comfort provided, they also pose severe privacy threats to both smart home inhabitants and bystanders [4].

Three principal strategies exist to mitigate privacy risks and to configure devices according to users’ preferences: (1) adapting device behavior through software settings; (2) physically disabling individual sensors; and (3) disconnecting devices.

Concerning the first strategy, software settings, we note that it foremost requires manufacturers to provide such control options. Also, it requires users to trust the device manufacturer in respecting their wishes as they have little control in knowing, for example, whether a microphone is actually still used to record audio or not. In contrast, the second option, physically disabling sensors, can provide such assurance [7]. Webcam shutters represent one of the most commonly known classes of physical interventions that are often integrated into modern camera-based smart home devices. Such covers can even be turned into smart devices that automatically block cameras when they are not in use [2]. Other examples include wearables that automatically deactivate nearby microphones [1] and a special hat that prevents smart speakers from listening [6]. Yet, they require additional external devices to configure the primary smart home device, rendering such solutions less usable for mass adoption. In summary, tangible smart device control is still mostly limited to built-in camera shutters [7].

The third option, disconnecting devices, applies to all smart home appliances. Users can always disconnect them from the network or turn off their power. While this represents the most effective strategy to mitigate privacy risks, it comes at the expense of losing device features and desired comfort, rendering this option typically unacceptable to most users. However, we note that there are several device connectivity options between complete *offline* and *online* modes, such as *access point* or *network-only* connections. Yet, smart home devices typically provide features only when being fully connected to the internet.

We developed ConnectivityControl, to depict how a smart home ecosystem that designs specifically for the four connectivity modes *offline*, *access point*, *network-only*, and *online*, can benefit users by giving them real smart home privacy configuration options that let them weigh comfort and privacy exposure. In this paper, we provide a detailed overview of the four connectivity modes, the two prototype devices, and the web interface.

Contribution Statement

We present a prototype system, ConnectivityControl, that increases the control of smart home end users over data sharing practices of their devices. This improvement in end-user privacy control is achieved in three ways: 1) by extending devices’ typical connectivity spectrum with *network-only* and *access point* modes; 2) by allowing end users to weigh between features and risks of devices across the connectivity spectrum; and 3) by introducing a tangible mechanism that is easy to use and interpret among smart home owners and bystanders. We discuss our vision of turning ConnectivityControl, with the support of manufacturers and the research community, into a larger smart home ecosystem that returns smart home privacy control to end users.

2 System

In this section, we first describe in detail the four connectivity modes and the ConnectivityLabel. Next, we present the two key components of ConnectivityControl: (1) the devices and their specific interfaces; and (2) the web platform. We conclude this section with an overview of the system architecture.

2.1 Connectivity Modes

Online refers to full internet access and represents the connectivity mode that most modern smart home devices require by default. Devices can send and retrieve data by communicating with remote web servers.

Network-only mode limits data exchange to devices that are within the same network. In a typical smart home with a single access point, this means that data can be shared across devices in this home, but should not leave the physical boundaries of the house. We note that assuring this desired communication behavior requires network devices that support package filtering and is increasingly difficult in more complex network setups.

Access point mode refers to the ability of a network device to set up its network interface specifically for direct connections with other devices. In most cases, data exchange on these network interfaces is limited to the connected communication partners. Some smart home devices use this mode for initial setup, allowing a user to connect with their mobile phone or computer to provide credentials for connecting to the home network. In contrast, ConnectivityControl foresees exchanging actual usage data during the device lifetime in this mode.

Offline means that a device cannot exchange any data over network interfaces. It does not use any cable or wireless network interface.





Connectivity	Features	Privacy Threats
Online	 Remote Diagnosis and Support	Remote device control and status tracking
Network-only	 Speech-based Preparation	Misuse and data intercept by close-by people with network access
Access point	 Advanced Settings	Third-party configuration
Offline	 Manual	None
Smart Coffee Maker TX2441 Label issued for Firmware Version 3.23.13b		

Fig. 1. The ConnectivityLabel informs users about the privacy/feature tradeoffs of each connectivity mode. A large icon in the *Features* column highlights features enabled by the corresponding connectivity level. We note that this is a prototypical label for a fictional device that will be refined through user testing.

2.2 ConnectivityLabel

Emami-Naeini et al. [3] proposed static device labels that detail principal security and privacy considerations of smart devices. The labels are expected to support users in making informed purchase decisions. Inspired by these, ConnectivityLabel revolves around the four connectivity modes and contrasts device features (i.e., comfort) with corresponding privacy implications and threats. Figure 1 depicts an example ConnectivityLabel for a fictional smart coffee maker.

2.3 Device Level

ConnectivityControl prescribes the following physical interfaces that must be implemented by devices within the ecosystem.

Four-State Switch As shown in Figure 2, each device must have a physical interface that shows the current connectivity mode of the device and that allows the user to change the mode. Four LEDs are used to visually highlight the currently active mode. The slider is positioned close to the corresponding LED. The motorized slider can either be manipulated manually by the user or programmatically be repositioned through ConnectivityControl’s web platform. This feature can be used when a device owner wants to remotely change device connectivity from *online* mode to any lower connectivity level. Note that programmatically switching back to a higher connectivity mode requires that the user has corresponding access to the device.

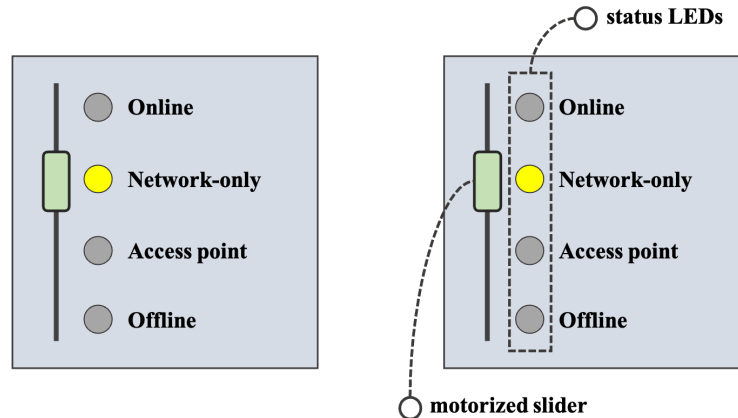


Fig. 2. Devices integrated into the ConnectivityControl ecosystem must feature a physical interface that allows changing between the four connectivity modes and that shows the current state.

QR Codes Each device is uniquely identifiable through a QR code attached to the device itself. This code is used to connect the specific device with the owner’s ConnectivityControl account. This private QR code is accessible only after opening the package of the device. In contrast, a second QR code publicly attached to the device package allows users to retrieve information about the device connectivity modes and corresponding features before purchasing the device. This takes inspiration from the static privacy and security labels proposed by Emami-Naeini et al. [3].

2.4 Web Platform

The React Native web platform enables ConnectivityControl device users foremost to create an account and to manage the devices they own. The platform is accessible on mobile devices and computers. After adding a device through the private and unique device QR code, users can always review the latest ConnectivityLabel associated with this device. In a future iteration, they are also expected to receive email notifications whenever a label associated with a user’s device gets updated to reflect new device features or adjusted privacy considerations.

In case a selected device is currently in *online* mode, the users can invoke the dedicated *online* devices features and lower the connectivity level.

2.5 Architecture

Figure 3 provides an overview of the key components introduced in this section and their interplay.

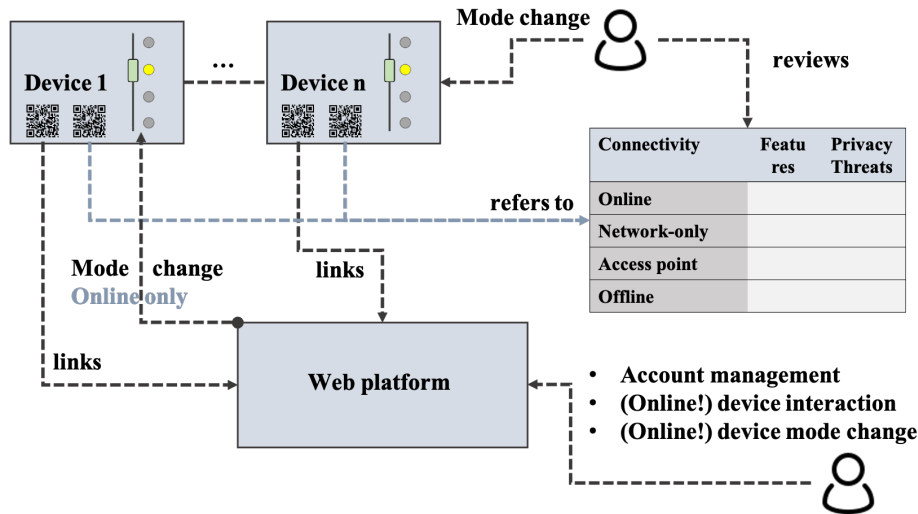


Fig. 3. High-level overview of ConnectivityControl’s system architecture.

We note that the web platform is the central hub for account management and provides device control features. However, the device management features are only available for devices that are in *online* mode at the time of platform interaction. Users can always review the ConnectivityLabel of devices, irrespective of their connectivity level and even before actual device purchase/registration. Further, users can always physically manipulate the connectivity level of smart home devices. The same is true on the web platform for *online* devices.

3 Prototypes

Currently, ConnectivityControl includes two prototype devices that showcase the different uses of diverse sensors across the connectivity spectrum. Figure 4 shows the environmental sensing unit and a camera module. Both prototypes are based on the popular low-cost WiFi microcontroller ESP32. The tangible connectivity user interface is based on a linear motorized potentiometer commonly used as a fader in mixing consoles.

In *offline* mode, the environmental sensing unit, shown on the left, displays the temperature and humidity on an integrated LED matrix. In any other mode, it transmits those data digitally. In *network* or *online* mode, the data can be used to control a connected off-the-shelves thermostat. The camera module, in the center, provides recordings on a removable SD card in *offline* mode. Recordings are transmitted according to the connectivity settings in the other three modes. The web interface of ConnectivityControl allows users to contrast features with risks for each corresponding device across the connectivity spectrum.

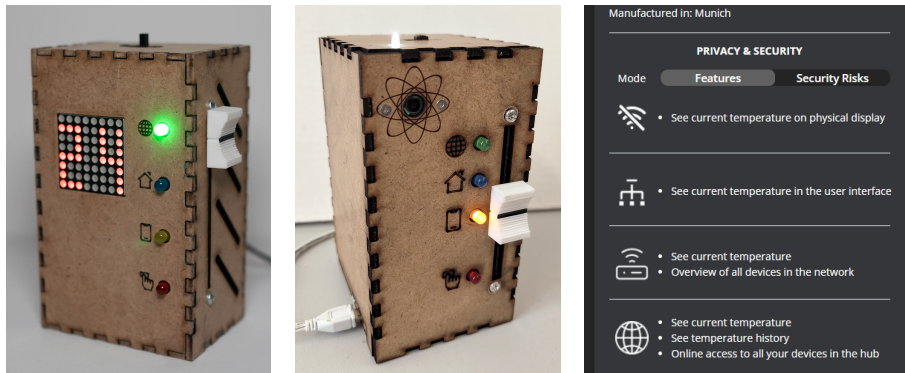


Fig. 4. The two prototype devices (left: environmental sensing unit; center: camera) share the same four-stage connectivity interface that characterizes ConnectivityControl. Right: The web interface shows the ConnectivityLabel for the environmental sensing unit, contrasting features and risks across the four connectivity levels.

Figure 5 depicts two web interface views, displayed on a mobile device. Users can select among their registered devices (left) for detailed information about

the smart home appliance and its data. In the case of the environmental sensing unit (right), the user can review temperature history for those periods in which the device was in *online* mode.

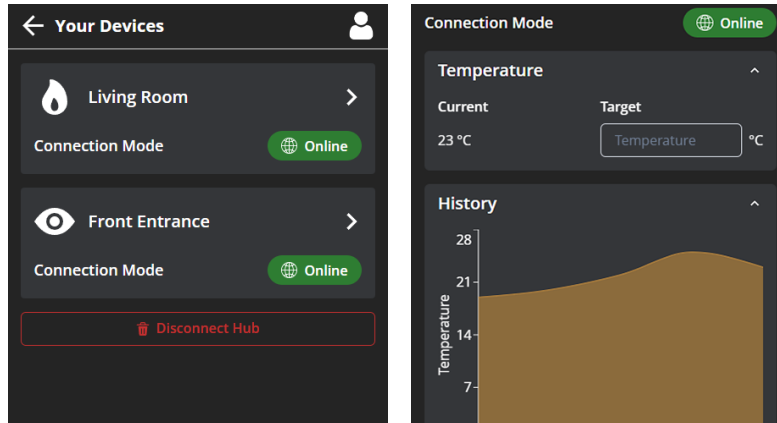


Fig. 5. Some of the principal views of ConnectivityControl’s web interface. Left: Overview of the registered devices and their connectivity states. Right: Detailed view of a selected device.

4 Discussion and Future Work

Smart home devices become increasingly attractive due to the multitude of features they provide. Yet, smart home inhabitants and bystanders typically have little control over these devices. Actually disconnecting them from the power outlet or the internet network remains in most cases the only real configuration option, rendering the devices useless. ConnectivityControl envisions an entirely new class of smart device configuration that is based on four network connection levels and clear ConnectivityLabels that allow users to weigh comfort and privacy implications. In this context, we note that the system focuses on TCP/UDP-based data exchange and does not currently consider additional communication schemes and technologies like service-based Bluetooth Low Energy or NFC.

Our latest prototype ecosystem features two devices: one ESP32-based camera and a smart thermostat with environmental sensors. We note that the user-centered development and evaluation of ConnectivityControl requires the future integration of additional device types and models that represent actual smart home configurations to the largest extent possible. Therefore, we hope that the presented physical and web prototypes will spark discussions and interest among device manufacturers and the research community, forming an initiative that develops smart home device ecosystems that highly value diverse device connectivity options. It will be particularly interesting to see how designers deal

with lower-than-usual connectivity, in particular *offline* modes. Related to the environmental sensing unit, we deal with this challenge by integrating a display. More complex devices like smart access control systems might need to integrate alternative physical mechanisms like manual locks as secondary interaction modalities.

Besides researching and integrating advanced built-in tangible sensor blockers, we consider the presented strategy highly promising for returning actual smart home privacy control to end users. While we commit to adding smart lighting systems and motorized window blinds to our ecosystem next, we hope for wider contributions from research and practice that will quickly allow running long-term studies on the adoption and use of connectivity-based smart home control systems.

In this context, we note the following user-centered requirements and opportunities for future work. First, extensive user testing will enable the design of a `ConnectivityLabel` that can be used uniformly across devices. This label must be intuitive for all smart home users and clearly allow weighing between features and risks in relation to the four connectivity levels. While the communication of device features, as illustrated in Figure 1, might be rather straightforward, the intuitive and detailed communication of privacy threats in such a label remains a research and design challenge. Related work on privacy and security labels [3, 5] focused mostly on providing a high-level assessment. Second, future work should explore actual `ConnectivityControl` user behavior in real smart homes and thoroughly document circumstances and motivations for interaction with the connectivity control interface. This includes dimensions such as the type of user initiating the change (i.e., smart home owner or bystander), the type of device, the origin of interaction (i.e., physical intervention or remote change through the web interface), and the social setting in which the change occurred. Based on the sum of findings from these user-centered research threads, we are confident that future smart home systems sharing control mechanisms as envisioned by `ConnectivityControl` and its associated `ConnectivityLabel` will be able to transform how smart home end users, i.e., owners and bystanders, weigh devices' features and risks and take informed decisions.

References

1. Chen, Y., Li, H., Teng, S.Y., Nagels, S., Li, Z., Lopes, P., Zhao, B.Y., Zheng, H.: Wearable microphone jamming. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. p. 1–12. CHI '20, Association for Computing Machinery, New York, NY, USA (2020). <https://doi.org/10.1145/3313831.3376304>, <https://doi.org/10.1145/3313831.3376304>
2. Do, Y., Park, J.W., Wu, Y., Basu, A., Zhang, D., Abowd, G.D., Das, S.: Smart webcam cover: Exploring the design of an intelligent webcam cover to improve usability and trust. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 5(4) (dec 2022). <https://doi.org/10.1145/3494983>, <https://doi-org.emedien.uni-muenchen.de/10.1145/3494983>

3. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into iot device purchase behavior. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. p. 1–12. CHI '19, Association for Computing Machinery, New York, NY, USA (2019). <https://doi.org/10.1145/3290605.3300764>, <https://doi.org/10.1145/3290605.3300764>
4. Obermaier, J., Hutle, M.: Analyzing the security and privacy of cloud-based video surveillance systems. In: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. p. 22–28. IoTPTS '16, Association for Computing Machinery, New York, NY, USA (2016). <https://doi.org/10.1145/2899007.2899008>, <https://doi.org/10.1145/2899007.2899008>
5. Oser, P., Feger, S., Woźniak, P.W., Karolus, J., Spagnuolo, D., Gupta, A., Lüders, S., Schmidt, A., Kargl, F.: Safer: Development and evaluation of an iot device risk assessment framework in a multinational organization. vol. 4, pp. 1–22. ACM New York, NY, USA (2020)
6. Tiefenau, C., Häring, M., Gerlitz, E., von Zezschwitz, E.: Making privacy graspable: Can we nudge users to use privacy enhancing techniques? (2019). <https://doi.org/10.48550/ARXIV.1911.07701>, <https://arxiv.org/abs/1911.07701>
7. Windl, M., Schmidt, A., Feger, S.S.: Investigating tangible privacy-preserving mechanisms for future smart homes (2023)