Centro Nazionale IOTePRIVACY

The new ETSI Standard on the "Cyber Security for Consumer Internet of Things": some legal thoughts on privacy, consent and UX

Giulio Messori, LL.M.

NGIoT e-Workshop
May 24th, 2019

A matter of time?

Product Security lifecycle
Provision 4.2-3: *Companies should* ***continuously monitor [...]*** also with the help of CVD - Coordinated Vulnerability Disclosure

A matter of time?

Product Security lifecycle
Provision 4.2-3: *Companies should **continuously monitor [...]*** also with the help of CVD - Coordinated Vulnerability Disclosure

Good to have a **system** with **periodic checks** on IoT devices

A matter of time?

Product Security lifecycle	
Provision 4.2-3: *Companies should* ***continuously monitor [...]*** also with the help of CVD - Coordinated Vulnerability Disclosure	
Vulnerabilities	
Provision 4.2-2: Disclosed vulnerabilities should be acted on in a timely manner. (Software fix)	*De facto* standard for the vulnerability process to be completed: **90 days**

A matter of time?

Product Security lifecycle	
Provision 4.2-3: *Companies should* ***continuously monitor [...]*** also with the help of CVD - Coordinated Vulnerability Disclosure	
Vulnerabilities	
Provision 4.2-2: Disclosed vulnerabilities should be acted on in a timely manner. (Software fix)	*De facto* standard for the vulnerability process to be completed: **90 days**
Reg. EU 679/2016 ("GDPR) provisions on breaches	
(**If you are the controller** in the IoT system) Notificate a personal data breach to the supervisory authority (Art. 33(1), GDPR)	"**Without undue delay** and, where feasible, **not later than 72 hours** after having become aware".
(**If you are the processor** in the IoT system) Notify the controller (Art. 33(2), GDPR)	"**Without undue delay** after becoming aware of a personal data breach".
Communicate a personal data breach to the data subject/subjects (Art. 34, GDPR)	When the personal data breach is **likely to result in a high risk**

4.8 Ensure that personal data is protected

Provision 4.8-1 Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

4.8 Ensure that personal data is protected

Provision 4.8-1 Device manufacturers and service providers shall provide consumers with **clear and transparent information** about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to **third parties** that can be involved, including advertisers.

Provision 4.8-2 Where personal data is processed on the basis of consumers' consent, this **consent shall be obtained in a valid way.**

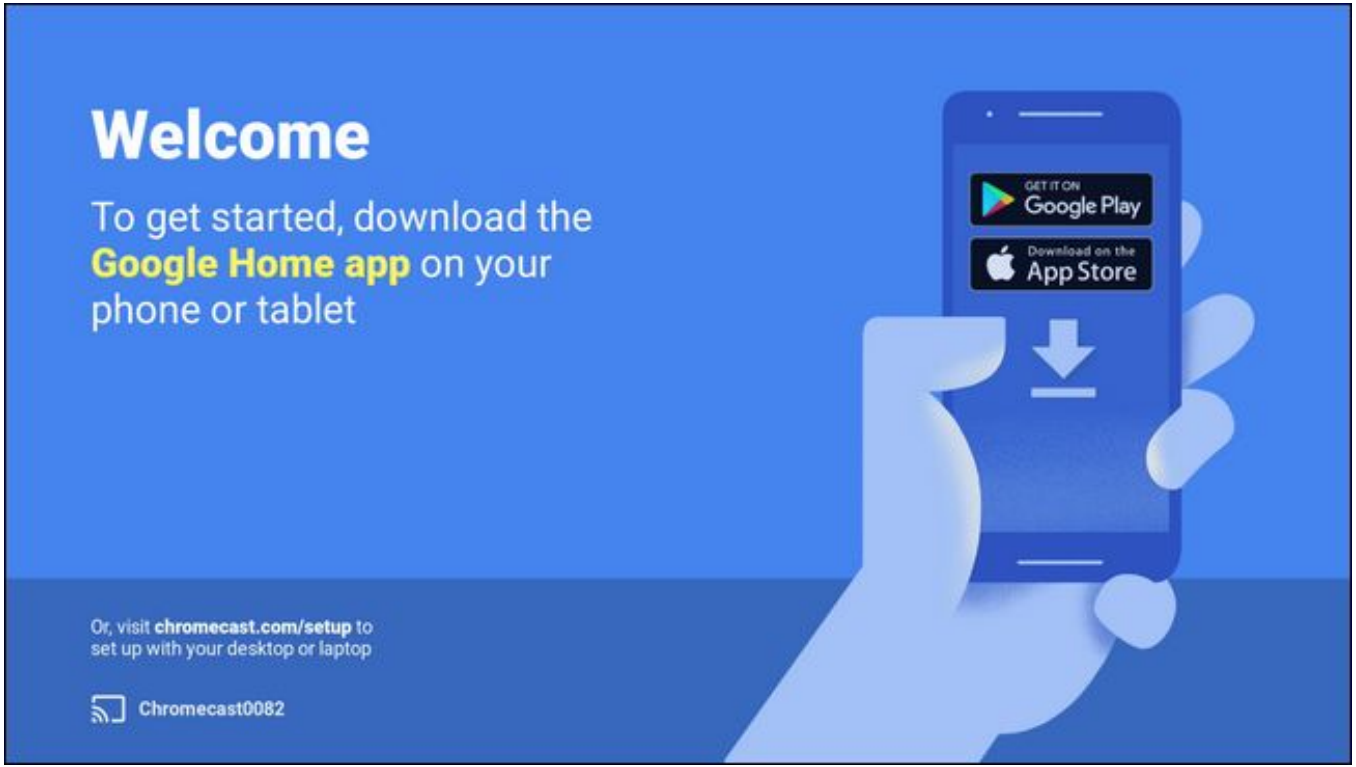
“Obtaining consent "in a valid way" normally involves giving consumers a **free, obvious and explicit opt-in choice** of whether their personal data can be used for a specified purpose.”

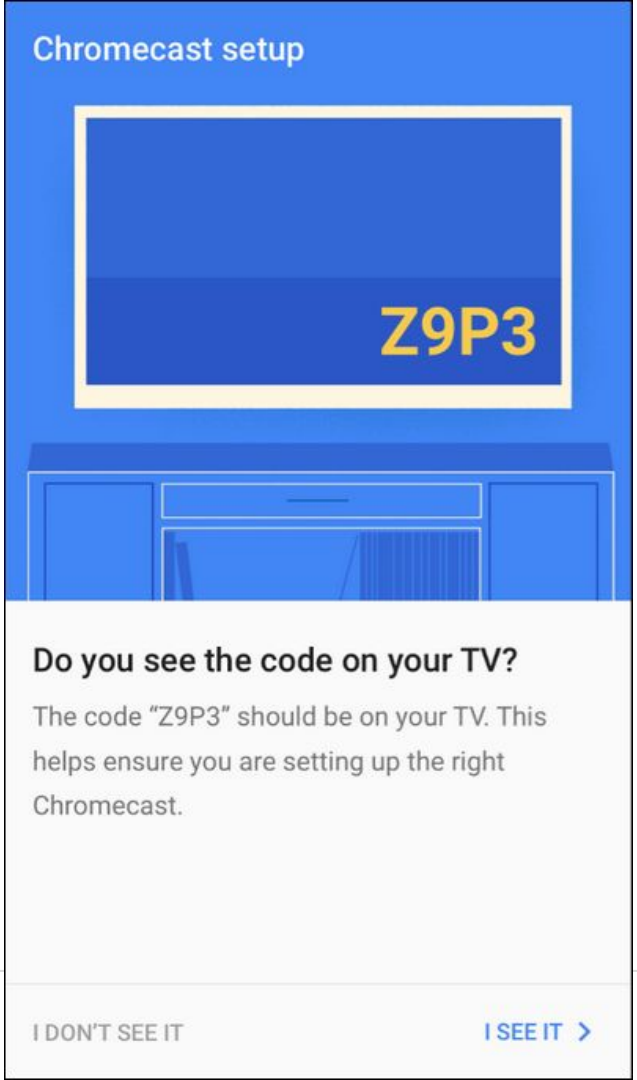
4.8 Ensure that personal data is protected

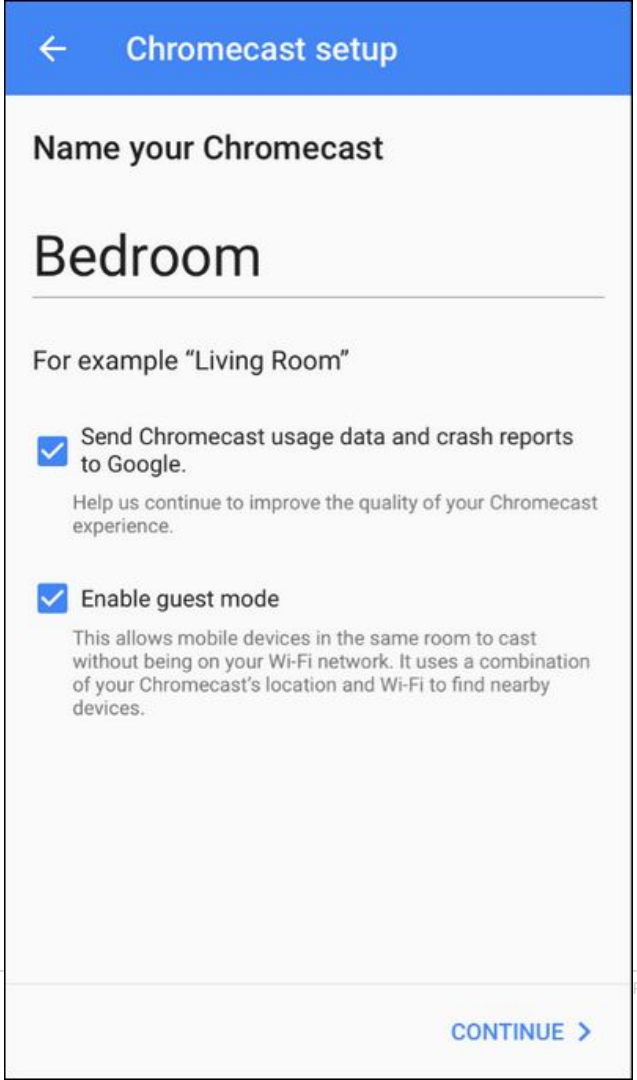
Provision 4.8-1 Device manufacturers and service providers shall provide consumers with **clear and transparent information** about how their

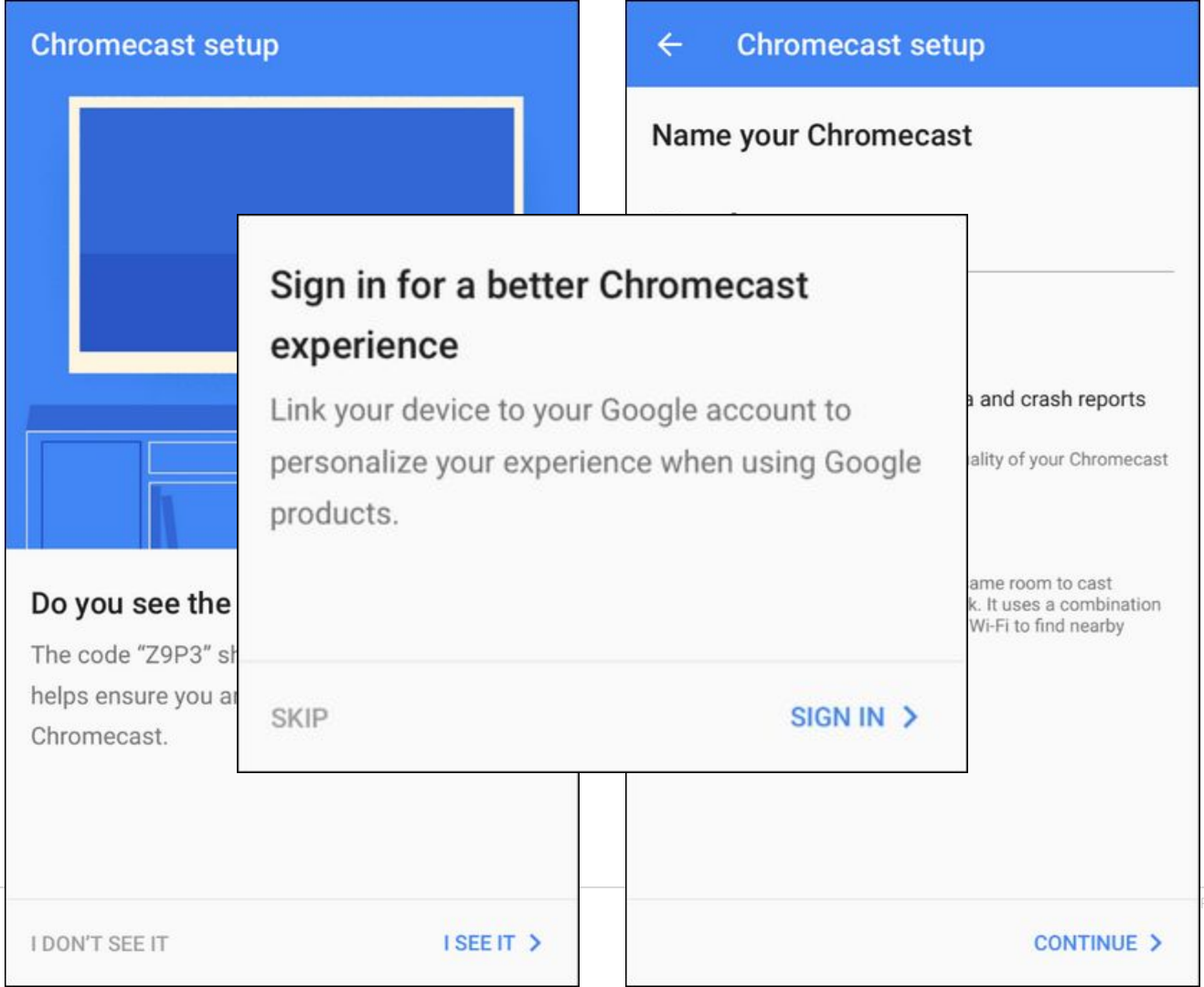
How to make sure that legal docs are “clear”, “transparent”, “obvious” and “explicit”?

free, obvious and explicit opt-in choice of whether their personal data can be used for a specified purpose.”


Welcome
To get started, download the Google Home app on your phone or tablet
GET IT ON Google Play
Download on the App Store
Or, visit chromecast.com/setup to set up with your desktop or laptop
Chromecast0082


Chromecast setup
Z9P3
Do you see the code on your TV?
The code “Z9P3” should be on your TV. This helps ensure you are setting up the right Chromecast.
I DON’T SEE IT
I SEE IT


Chromecast setup
Name your Chromecast
Bedroom
For example “Living Room”
Send Chromecast usage data and crash reports to Google.
Help us continue to improve the quality of your Chromecast experience.
Enable guest mode
This allows mobile devices in the same room to cast without being on your Wi-Fi network. It uses a combination of your Chromecast’s location and Wi-Fi to find nearby devices.
CONTINUE


Chromecast setup
Do you see the
The code "Z9P3" sh
helps ensure you ar
Chromecast.
I DON'T SEE IT
I SEE IT
Sign in for a better Chromecast experience
Link your device to your Google account to personalize your experience when using Google products.
SKIP
SIGN IN
Chromecast setup
Name your Chromecast
and crash reports
ality of your Chromecast
ame room to cast
k. It uses a combination
Wi-Fi to find nearby
CONTINUE

Proving that **setup and legal docs acceptance** was made by parents

Still a “smart” toy?

What if there is no UX to interact with but the toy is still connected in some way?

4.8 Ensure that personal data is protected

Provision 4.8-3 Consumers who gave consent for the processing of their personal data shall be given the **opportunity to withdraw it** at any time.

Consumers expect to be provided with means to preserve their privacy by means of configuring IoT device and service functionality appropriately.

"Setting" sections?
Links or QR codes to a dedicated webpage?

What if there is no screen UX?

With **thousands and thousands** of IoT devices sold, come big headaches.

→ Consent management softwares ←


Privacy
Consumer
Law

A summary of the documents that shall be drafted

→ **Privacy Policy**
- \+ Various checkboxes
- \+ Pages on Data Protection rights

→ **Terms and Conditions**:
- Clauses on updates (Chapter 4.3);
- Clauses on basic functioning of the device and minimum availability during updates;
- Replacement plan and support;
- End-of-life policy.

\+ **Q/A on security issues** (e.g. ch. 4.4, 4.5, 4.9)

A summary on possible options for showing legal documents

1) Offline, before delivering the IoT product (**negotiation**);
2) Offline, in the **package**;
3) Online, thanks to a thoughtful in-app UX that guides the user step-by-step;
4) Online, with a QR code or link in the package that brings to a web page.