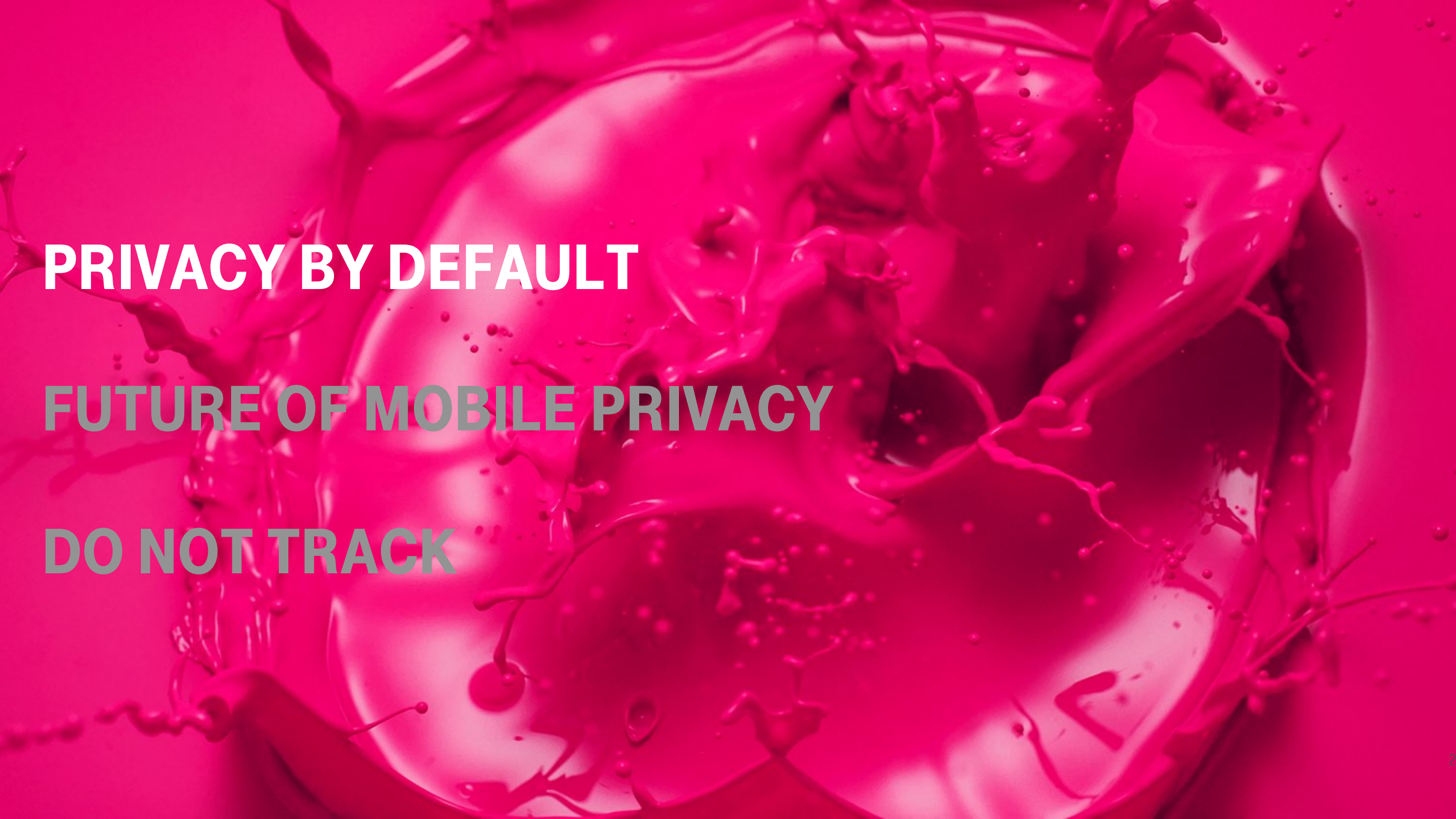
PRIVACY BY DEFAULT AND BEYOND

ERLEBEN, WAS VERBINDET.

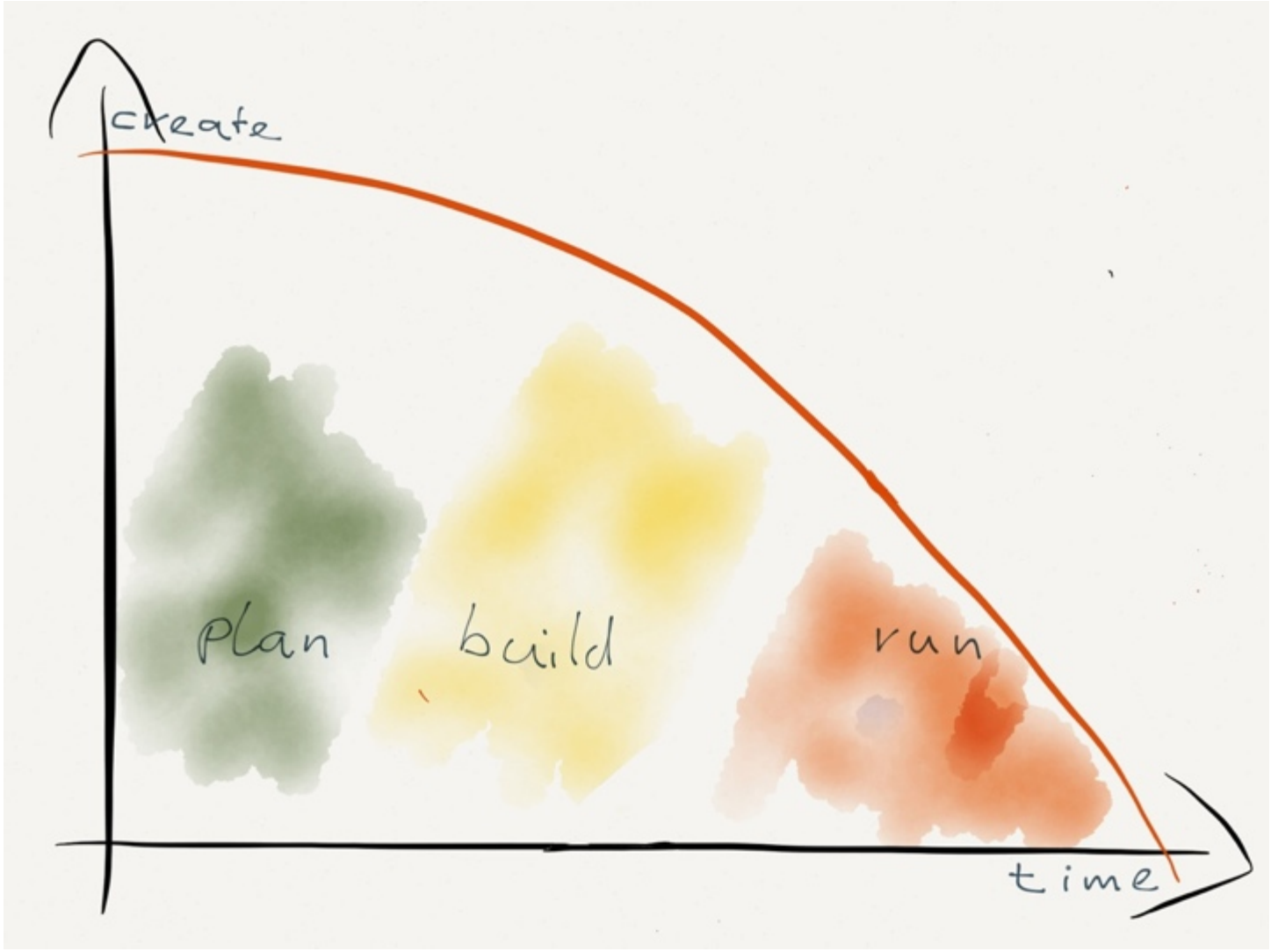

PRIVACY BY DEFAULT
FUTURE OF MOBILE PRIVACY
DO NOT TRACK

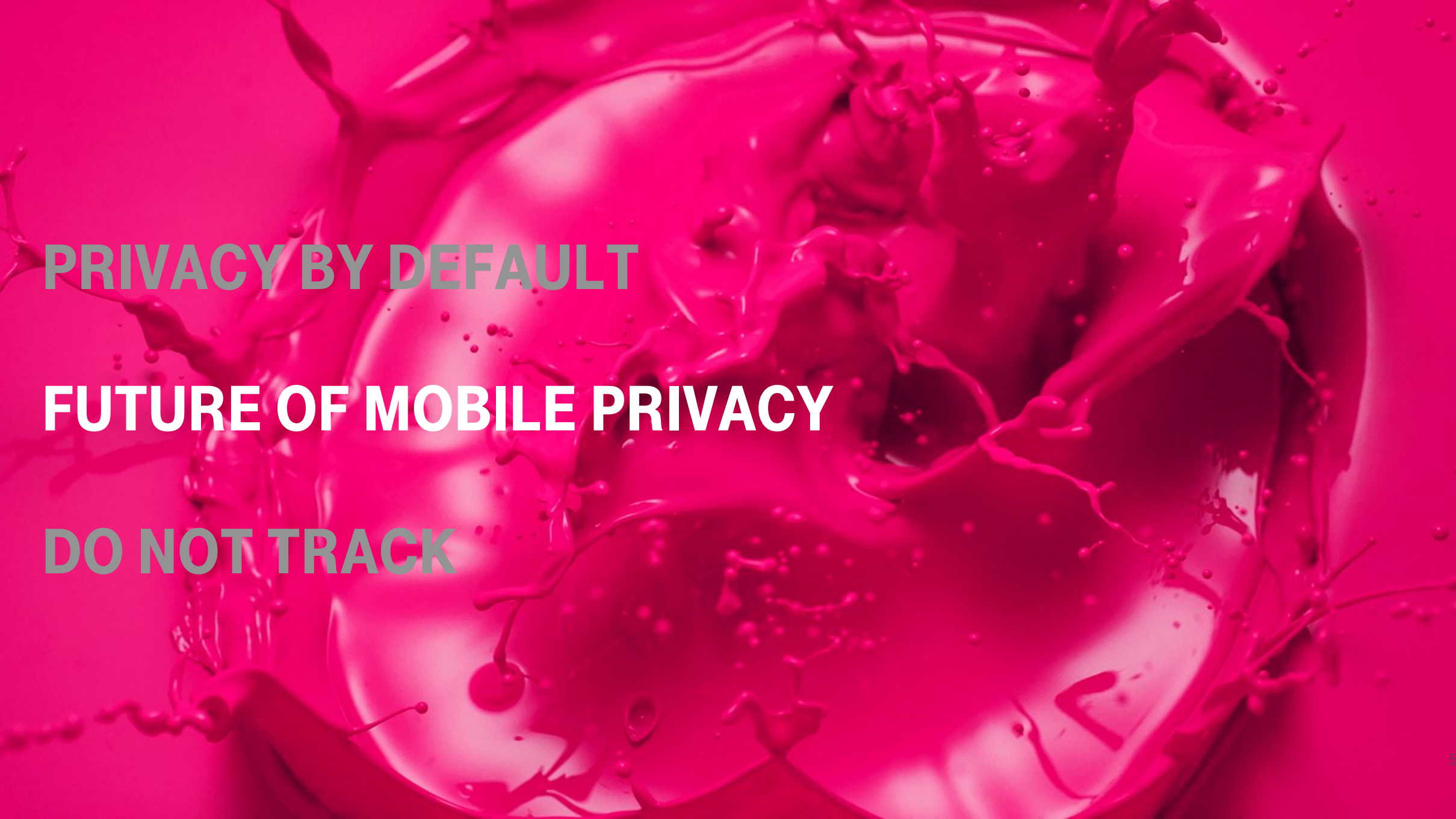
PRIVACY BY DESIGN PRINCIPLES

1) Proactive not reactive
2) Privacy as Default
3) Privacy embedded into design
4) Full functionality – positive sum, not zero-sum
5) End-to-end-security - lifecycle protection
6) Visibility and Transparency
7) Respect for User Privacy

Creating areas of trust !

FRÜHZEITIGE BETEILIGUNG IST UNABDINGBAR




PRIVACY BY DEFAULT
FUTURE OF MOBILE PRIVACY
DO NOT TRACK

OPTIMALER SCHUTZ DER PRIVATSPHÄRE AUF SMARTPHONES

Die Deutsche Telekom und Mozilla arbeiteten von 2013 - 2015 gemeinsam am Projekt „The Future of Mobile Privacy“

Ziel war die Entwicklung einfacher, effektiver und benutzergesteuerter Datenschutzfunktionen für mobile Geräte und die Unterstützung der Nutzer bei eigenen informierten Entscheidungen.

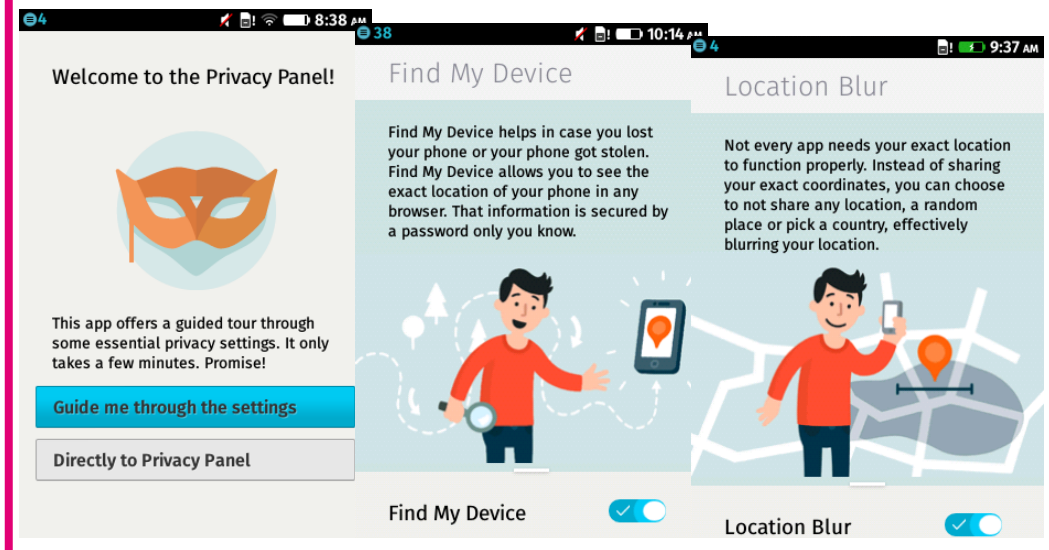
VOM PROTOTYPEN ZUM FIREFOX OS RELEASE

- **Beim Prototypen waren viele Funktionen nur visuell, jedoch nicht bzw. stark eingeschränkt funktional implementiert.**
- **Abhängigkeiten und Zusammenhänge mit anderen Funktionen konnten vernachlässigt werden.**
- **Bei der Realisierung der Funktionen für das Firefox OS Release waren deswegen die folgenden Punkte zu erfüllen:**
  - Um- bzw. Neuprogrammierung von Features (Prototyp B2G Version 1.4; Release B2G Version 2.1)
  - Erfüllung der Qualitätsanforderungen von Mozilla
  - Abstimmungen mit den Verantwortlichen bei Mozilla
  - Realisierung mit sehr schlankem Budget
  - Dynamische Timelines

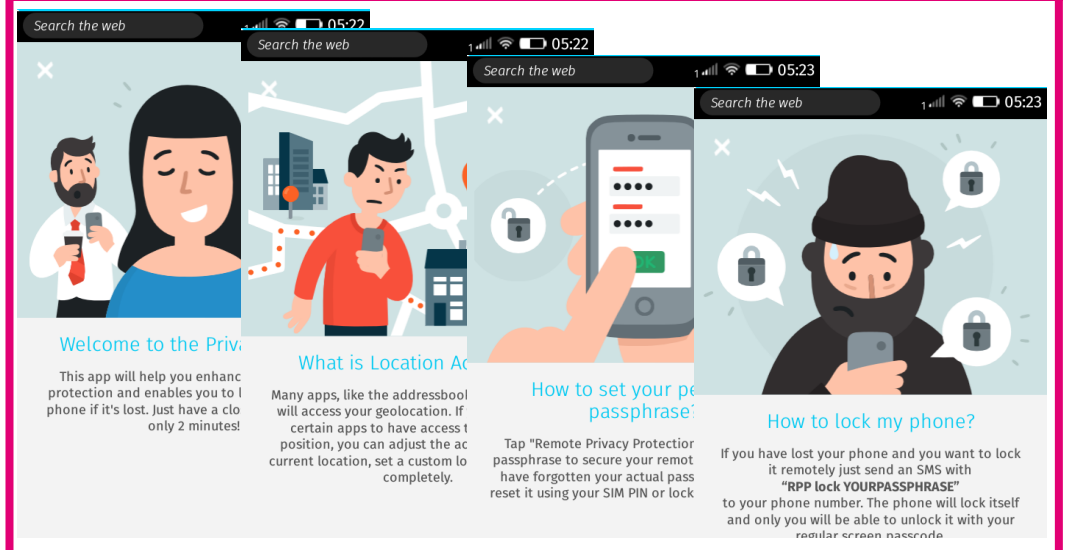
VOM PROTOTYPEN ZUM FIREFOX OS RELEASE

PRIVACY TOUR

Prototyp



Firefox OS Release 2.1 (Q2/2015)

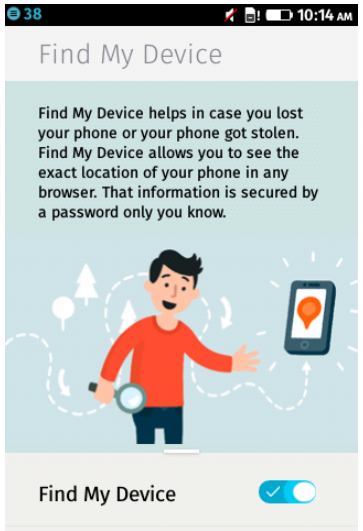


Die Guided Tour umfasst derzeit nur eine Beschreibung der neuen Features. Eine unmittelbare Verknüpfung mit den Einstellungsmöglich-keiten hatte zu große Implikationen mit dem gesamten Betriebssystem und war für das Firefox OS Release 2.2 (H2/2015) geplant.

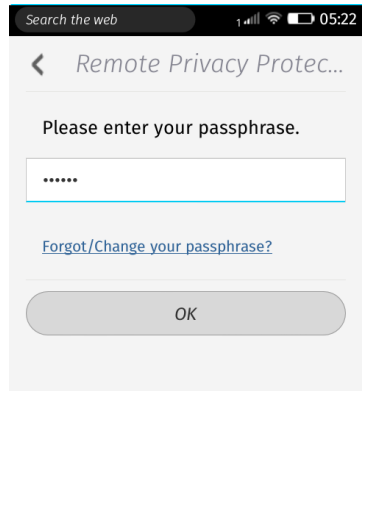
VOM PROTOTYPEN ZUM FIREFOX OS RELEASE

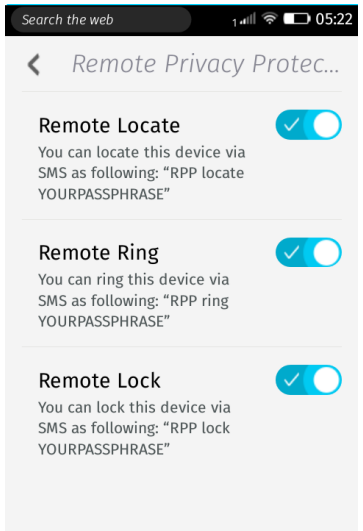
REMOTE PRIVACY PROTECTION

Prototyp



Firefox OS Release 2.1 (Q2/2015)



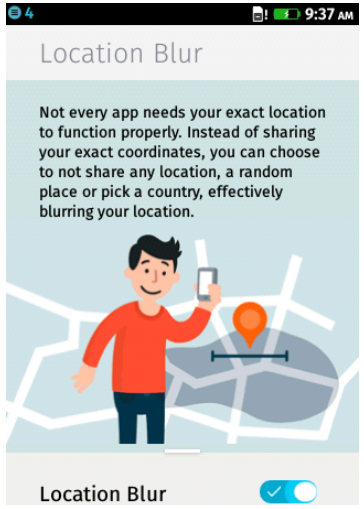


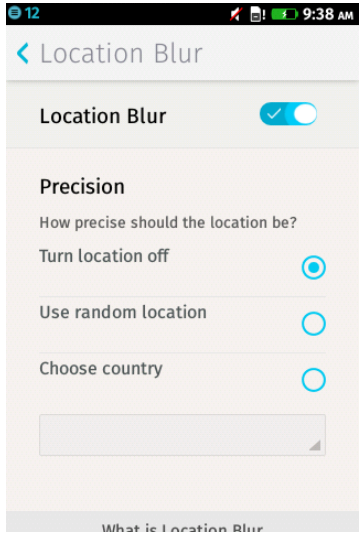
Implementiert wurde die Funktion für die Lokalisierung des Smartphone, basierend auf einem auf dem Gerät hinterlegten Passwort. Dieses Passwort wird per SMS mit einem entsprechenden Befehl an des verlorene Smartphone gesendet. Somit kann das Smartphone geortet werden, einen Ton abspielen und gesperrt werden. Auf einen Löschbefehl wurde verzichtet, weil keine Backup Funktion verfügbar war.

VOM PROTOTYPEN ZUM FIREFOX OS RELEASE

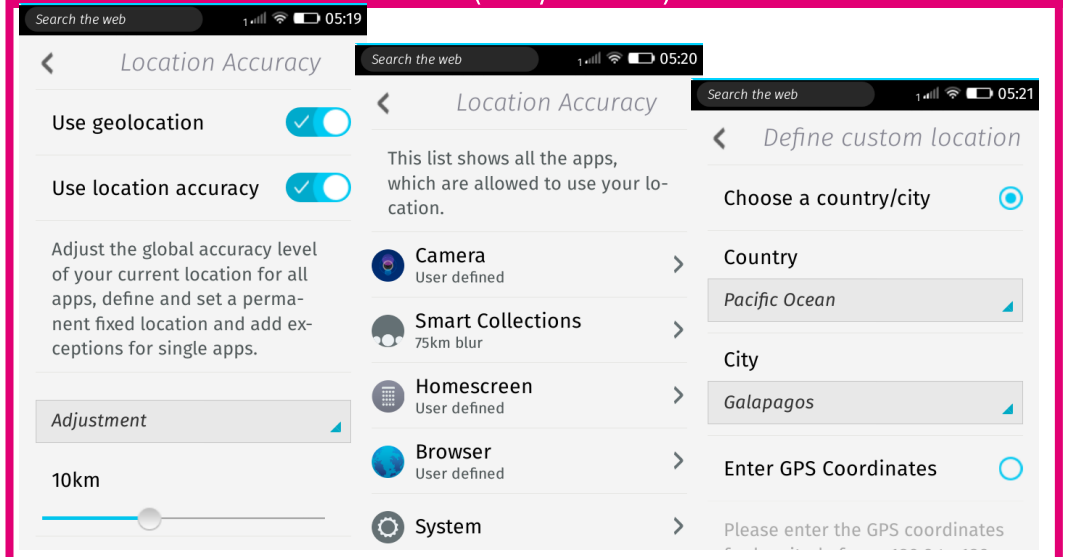
LOCATION ACCURACY

Prototyp

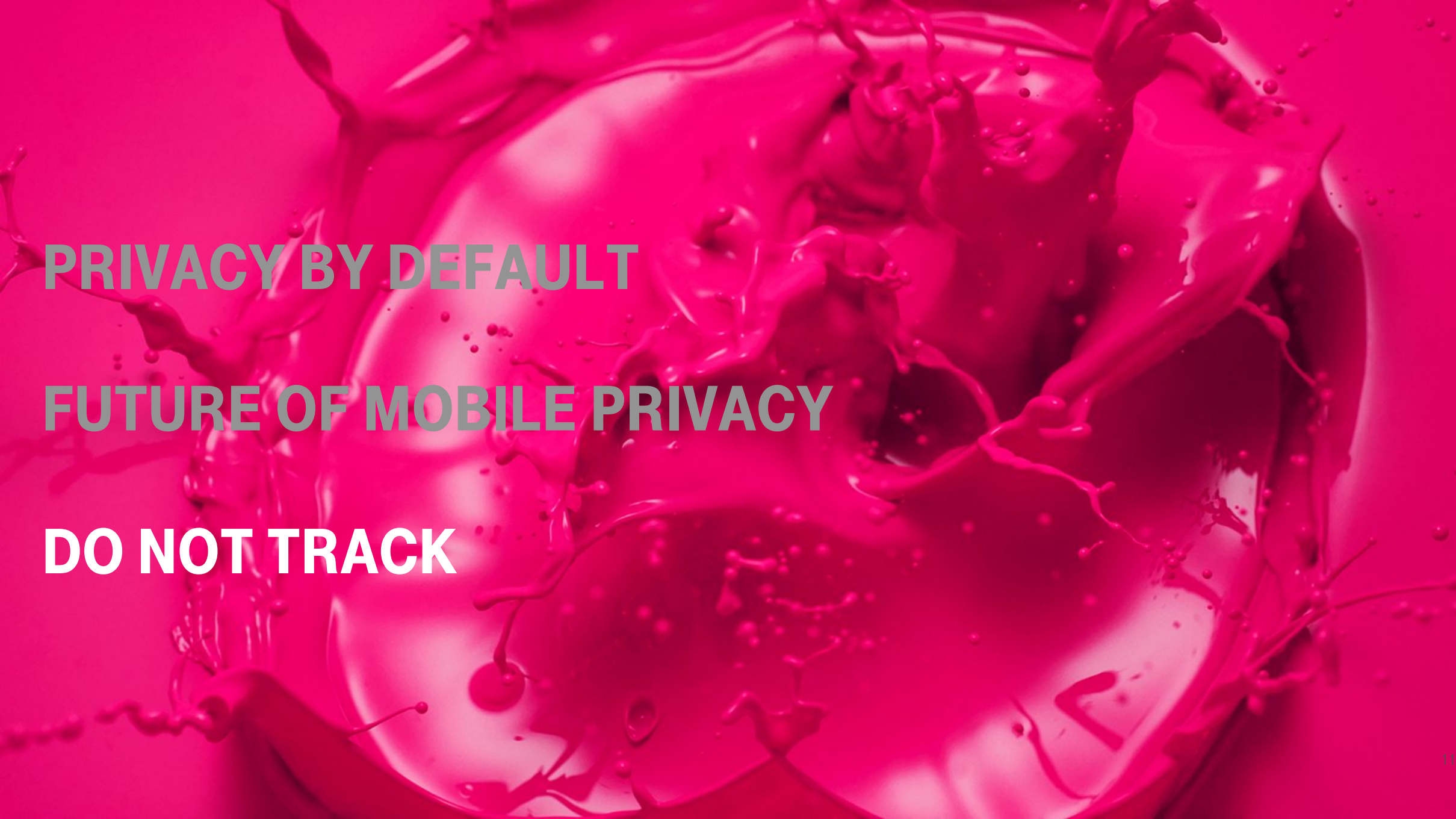




Firefox OS Release 2.1 (Q2/2015)



Gegenüber dem Prototypen wurde die Einstellungsmöglichkeit Lokalisierung stark überarbeitet. Hinzu gekommen ist die Möglichkeit – neben einer globalen Voreinstellung - je App festlegen zu können, wie genau die Lokalisierung erfolgen soll. Darüber hinaus wurde ein Algorithmus entwickelt, der die Verfremdung der Standortdaten realisiert. Die Lösung lässt sich auch auf andere Plattformen übertragen (z.B. Browser)


PRIVACY BY DEFAULT
FUTURE OF MOBILE PRIVACY
DO NOT TRACK

W3C TRACKING PROTECTION WORKING GROUP

66 group participants,

6 Invited Experts,

8 Working Group face to face meetings (2011 – 2013),

1 Global Considerations Task Force face to face meeting (2013)

Lots of regular teleconferences,

Tons of emails on the mailing list

Three direction approach:

- Tracking Preference Expression (technical spec)

no consensus:

- Tracking Compliance and Scope (compliance spec)
- Tracking Selection Lists

https://www.w3.org/2011/tracking-protection/

DNT - ACTUAL RESULTS OF THE W3C STANDARDIZATION: TECHNICAL SPECIFICATION

Tracking Preference Expression (DNT)
W3C Candidate Recommendation 07 September 2017
https://www.w3.org/TR/2017/CR-tracking-dnt-20170907/

This specification defines the DNT request header field as an HTTP mechanism for expressing the user's preference regarding tracking, an HTML DOM property to make that expression readable by scripts, and APIs that allow scripts to register site-specific exceptions granted by the user. It also defines mechanisms for sites to communicate whether and how they honor a received preference through use of the Tk response header field and well-known resources that provide a machine-readable tracking status.

DNT	meaning
1	This user prefers not to be tracked on the target site.
0	This user prefers to allow tracking on the target site.

DO NOT TRACK IS NOT PRIVACY BY DEFAULT !

Tracking Preference Expression (DNT)
W3C Candidate Recommendation 07 September 2017

...

10.1 Why DNT:1 is Not Preconfigured by Default

This specification defines a protocol for communicating the user's tracking preference, not a protocol that prevents tracking on its own. It might be tempting to assume that design for privacy would justify calling for DNT:1 to be preconfigured as the default for all user agents. However, that would violate the field's semantics, make its presence in a request meaningless, and add eight extra bytes to every HTTP request (with no effect).

The DNT signal alone does nothing to enhance a user's privacy. It is only when recipients believe that the signal has been deliberately and knowingly configured, and not defined as a default, that they will consider it to be the user's preference. Furthermore, when no signal is sent, recipients remain subject to whatever regulatory, legal, or other regional requirements regarding tracking exist in the absence of consent.

EINWILLIGUNG STATT BLOCKING / OPT-OUT

Photo: Daniel R. Blume https://www.flickr.com/photos/drb62/

Do not track bietet 2 Elemente:

1. Einen Schalter, der die Wünsche der Nutzer zum Umgang mit ihren Daten repräsentiert
2. Einen Mechanismus, der es Websites / Services ermöglicht mit den Nutzern zu kommunizieren

Was wäre, wenn diese beiden Elemente als Einwilligungsmechanismus, anstatt als Blockingmechanismus genutzt werden ?

Zusammenfassung:

Privacy by Default braucht Privacy by Design

Future of mobile privacy als Beispiel, dass existierende Privacy by Default Mechanismen neu gedacht werden müssen (und können)

Do Not Track ist nicht Privacy by Default, aber Einwilligung und Dialog mit dem Nutzer

Frank Wagner

frank.wagner@telekom.de