

# Privacy by Design

Integrating privacy by design in the software development lifecycle.

# Bart van Buitenen

- Managing Director Dasprive vzw
- Host Dasprive podcast
- CISO, DPO, consultant Data Protection & Security
- Lecturer Data Protection & Security  
Thomas More University
- Chair of the Flemish Committee for the  
Exchange of Personal Data
- LinkedIn or via <https://dasprive.be>



# Windows now includes Keylogger

- Microsoft Recall is a new “feature” for Windows
- Takes screenshots every three seconds and classifies anything you see or type via OCR / Azure AI (local)
- At least 3 months (25GB) & instantly indexed/searchable

## How the new Microsoft Recall feature fundamentally undermines Windows security



Kevin Beaumont · [Follow](#)

Published in DoublePulsar · 4 min read · May 21, 2024



323



8



Yesterday, Microsoft CEO Satya Nadella sat down with the media to introduce a new feature called Recall, as part of their Copilot+ PCs. It takes screenshots of what you're doing on constantly, by design:

# Windows now includes Keylogger

- Microsoft Recall is a new “feature” for Windows
- Takes screenshots every three seconds and classifies anything you see or type
- 3 months (25GB) & instantly indexed/searchable
- This includes anything anyone shows on your screen (meeting), messages, etc.
- Stored in plain text, easily extracted (TotalRecall)
- Access screenshots from another user? L33t h4cks engaged -> C:/Users



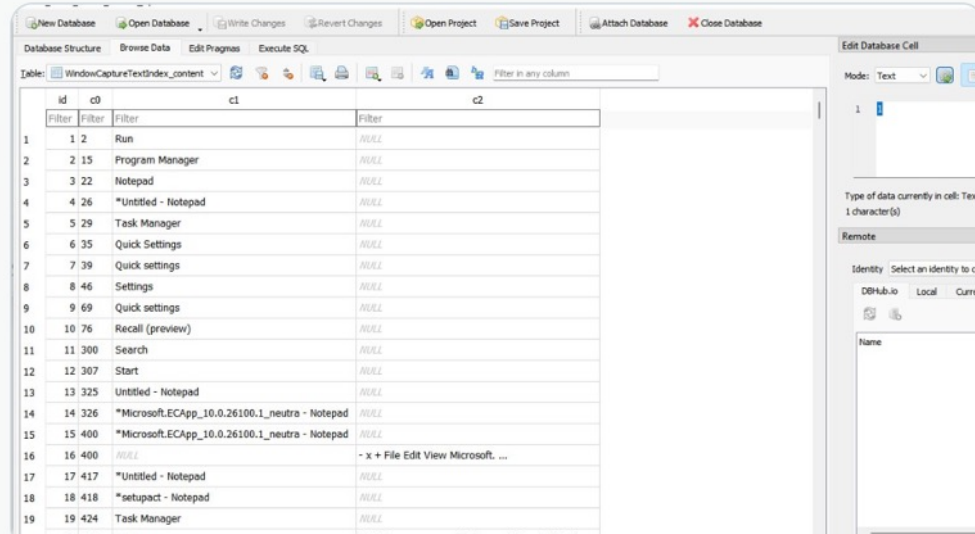
Kevin Beaumont   
@GossiTheDog · Follow



Microsoft told media outlets a hacker cannot exfiltrate Copilot+ Recall activity remotely.

Reality: how do you think hackers will exfiltrate this plain text database of everything the user has ever viewed on their PC? Very easily, I have it automated.

HT detective



id	c0	c1	c2
1	2	Run	NULL
2	15	Program Manager	NULL
3	22	Notepad	NULL
4	26	*Untitled - Notepad	NULL
5	29	Task Manager	NULL
6	35	Quick Settings	NULL
7	39	Quick settings	NULL
8	46	Settings	NULL
9	69	Quick settings	NULL
10	76	Recall (preview)	NULL
11	300	Search	NULL
12	307	Start	NULL
13	325	Untitled - Notepad	NULL
14	326	*Microsoft.ECApp_10.0.26100.1_neutra - Notepad	NULL
15	400	*Microsoft.ECApp_10.0.26100.1_neutra - Notepad	NULL
16	400	NULL	- x + File Edit View Microsoft. ...
17	417	*Untitled - Notepad	NULL
18	418	*setupact - Notepad	NULL
19	424	Task Manager	NULL
20	424	NULL	X O Type a name, publisher, or PID ... End task ...

6:34 PM · May 30, 2024



6.2K



Reply



Copy link

Read 118 replies

# Do we need privacy by design?

- The privacy paradox is real.
  - Power balance
  - Peer pressure
  - Necessity vs. Choice
  - Priorities
- But the onus shouldn't be on the user
- Enter privacy by design: now a legal requirement.



The privacy paradox: why do people keep using tech firms that abuse their data?

*John Naughton*

Despite privacy scandals, Facebook is more profitable than ever  
- journalists must use the tools of tech to understand why



▲ Mark Zuckerberg announcing new Facebook privacy features in San Jose, 30 April. But do most people care either way? Photograph: Amy Osborne/AFP/Getty Images

A   data security shadow looms over our networked world. It's called the "privacy paradox". The main commercial engine of this world involves erosion of, and intrusions upon, our privacy. Whenever researchers, opinion pollsters and other busybodies ask people if they value their privacy, they invariably respond with a resounding "yes".

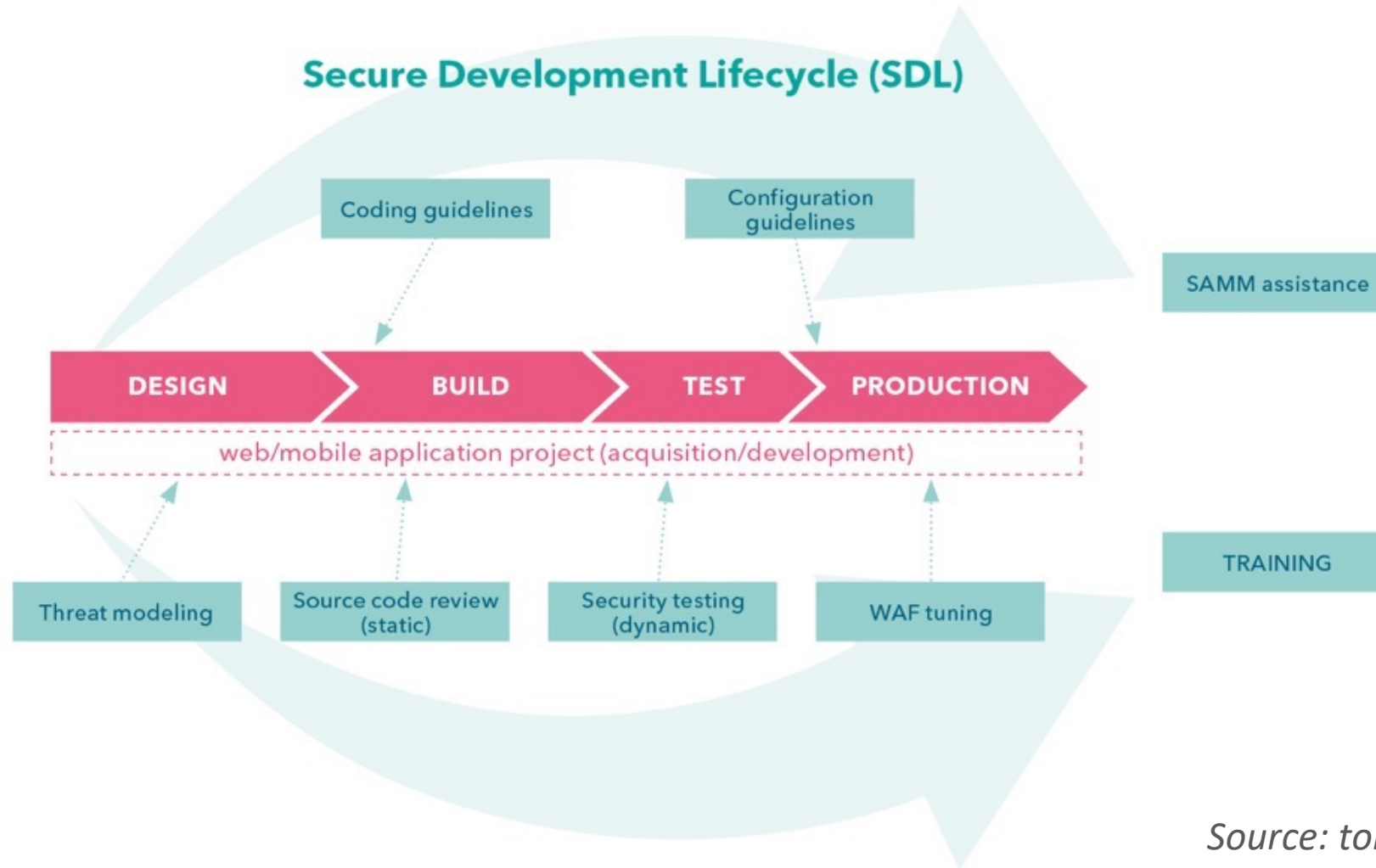
# Privacy by design

*Recital 4 GDPR: The processing of personal data should be designed to serve mankind.*

Privacy by design:

- A principle or intent to include privacy as a basic element into all processes of an organization involved with personal data
- It is not a separate topic, software feature or project: privacy is included as a basic requirement in anything that is made or designed
- When talking about software development, this means looking at all different stages of a project to incorporate privacy, and especially the start

# Integrating PbD into the SDL



Source: [toreon.com](http://toreon.com)

# Design.

- Privacy Threat modeling: data flow, identify threats, propose mitigations
  - Transparency, purpose, necessity & data minimization, storage, accuracy, security
- Features, design/UI/structure, physical setup
- Training & awareness project/dev team
  - Data Protection Impact Assessment?





# Develop / Build.

- May not always require input at this stage.
- But in this phase software security requirements = privacy requirements
- For example:
  - Test data (sometimes developers test)
  - Secure development guidelines
  - Code review
  - Documentation (accountability principle)



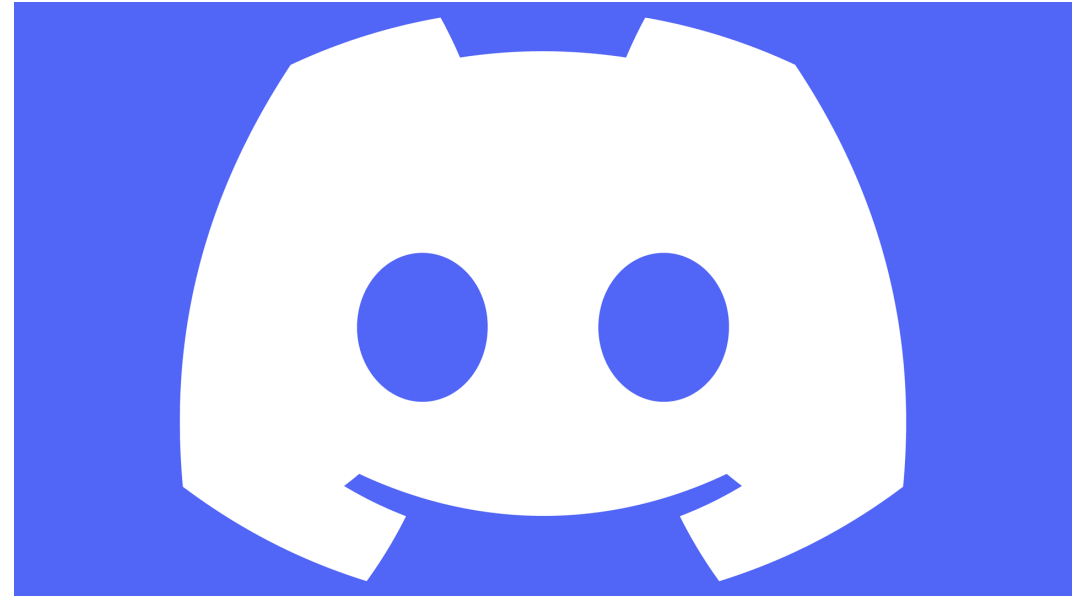
# Test.

- Whether digital or non-digital project: time to test it.
- For example
  - Test logging function
  - Defaults in the app
  - DSRs: access, portability



# Example: Discord

- Received a 800k fine by the CNIL
- Why?
  - 2.4 million user accounts that had not been used in over 3 years
  - Default behavior: clicking X (macOS vs windows)
  - Password of 6 characters accepted
  - No DPIA carried out



# Production / Deployment.

- Trust, but verify.
- Examples
  - Similar to Test phase, but for real
  - User feedback
  - Regression testing



# Governance.

- Doing the activities as described previously is great but needs to be part of a larger process.
- Privacy by Design also means implementing this on an organizational level.
- Management involvement, culture, privacy champions

Examples: PrivSec team, CAB, Project kick-off, Approval process



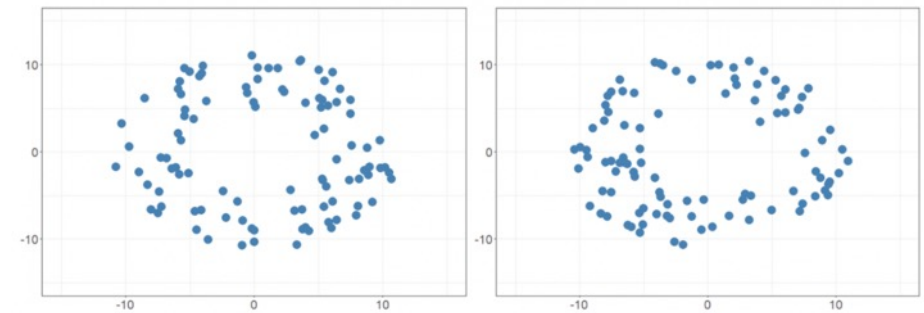
# What's the ROI?

- Better software = \$\$
  - Code quality
  - Security risks
- Better documentation
- Trustworthy reputation
- Happy customers
- Happy developers



# PETs

- Synthetic data (testing)



Original data

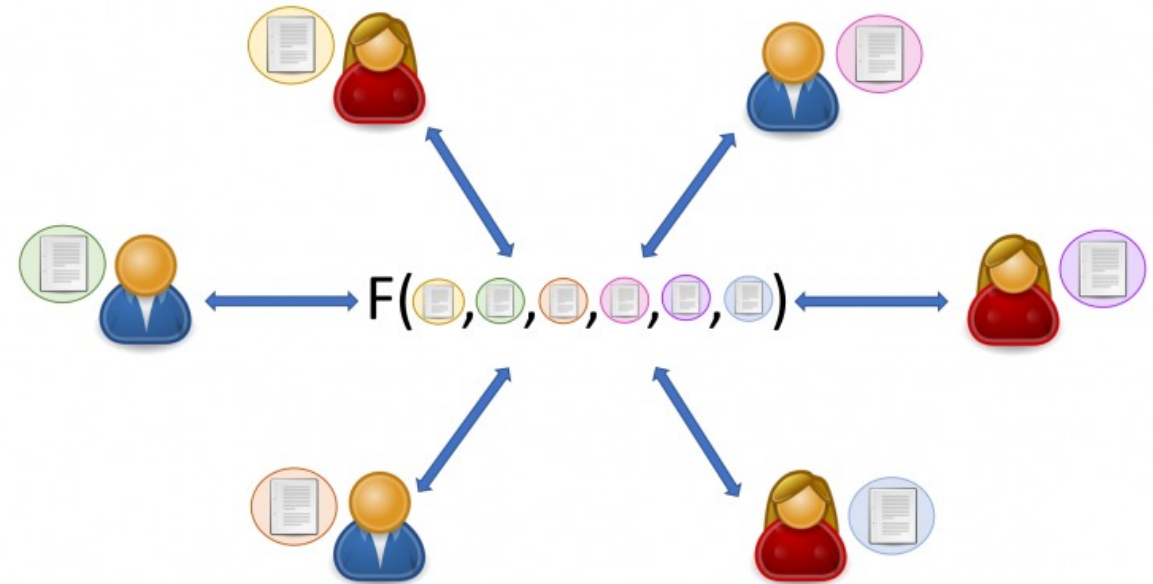
Synthetic data

The synthetic data retains the structure of the original data but is not the same

<https://dataingovernment.blog.gov.uk/2020/08/20/synthetic-data-unlocking-the-power-of-data-and-skills-for-machine-learning/>

# PETs

- Synthetic data (testing)
- Multiparty computation (design)

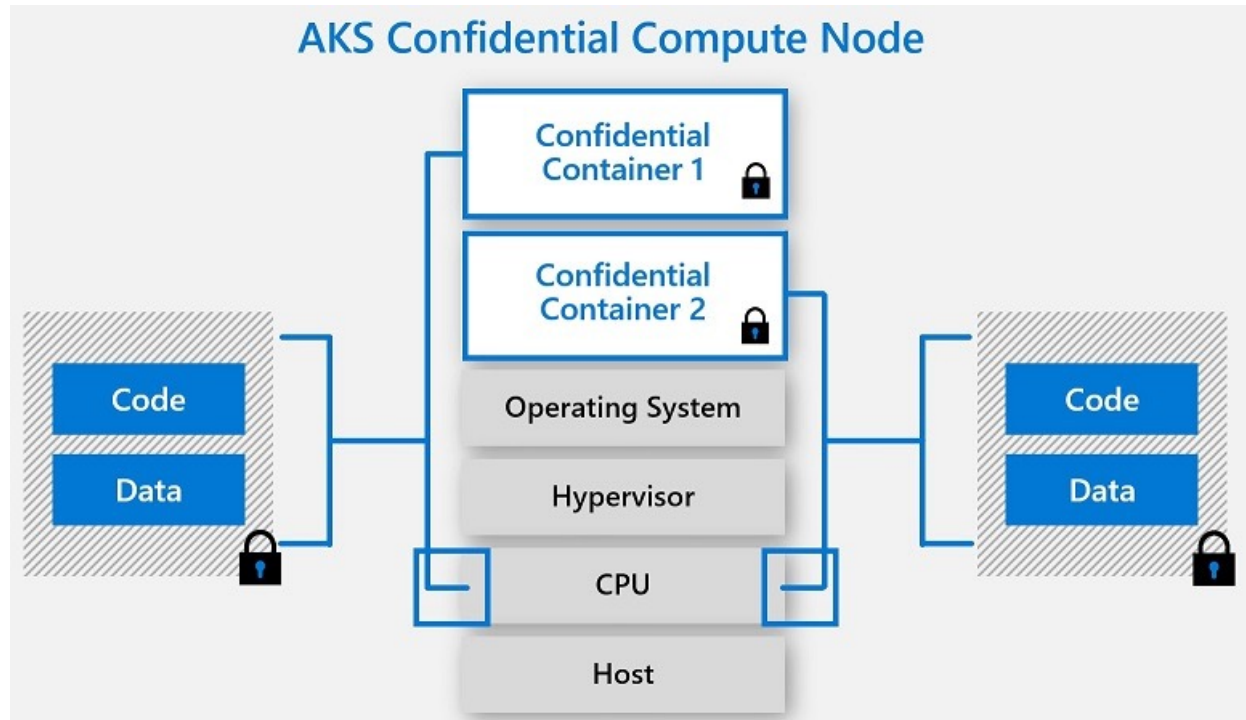


<https://www.esat.kuleuven.be/cosic/blog/the-three-musketeers-of-secure-computation-mpc-fhe-and-fe/>



# PETs

- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)



<https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-nodes-aks-overview>

# PETs

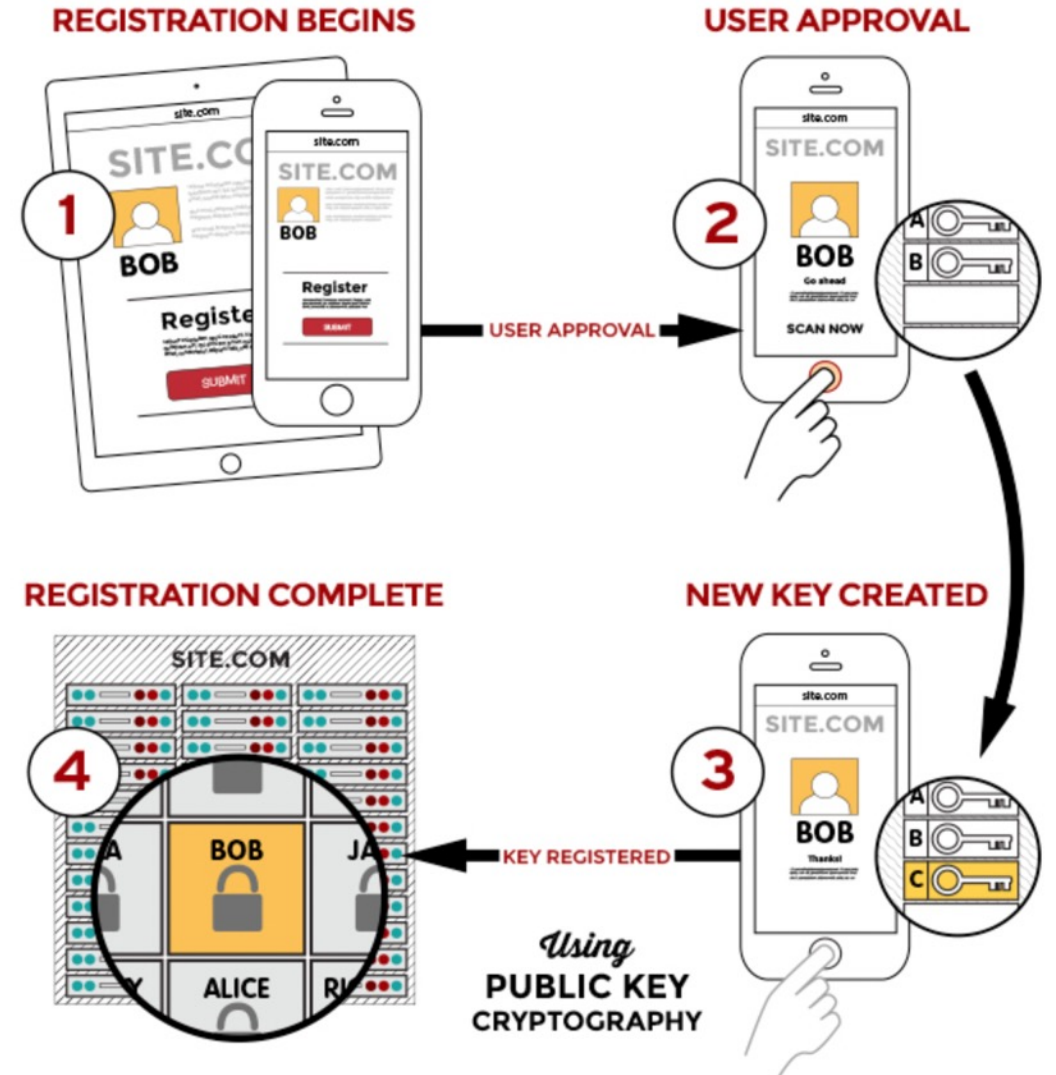
- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)



<https://www.qualcomm.com/news/onq/2017/08/we-are-making-device-ai-ubiquitous?cmpid=oofyus181544>

# PETs

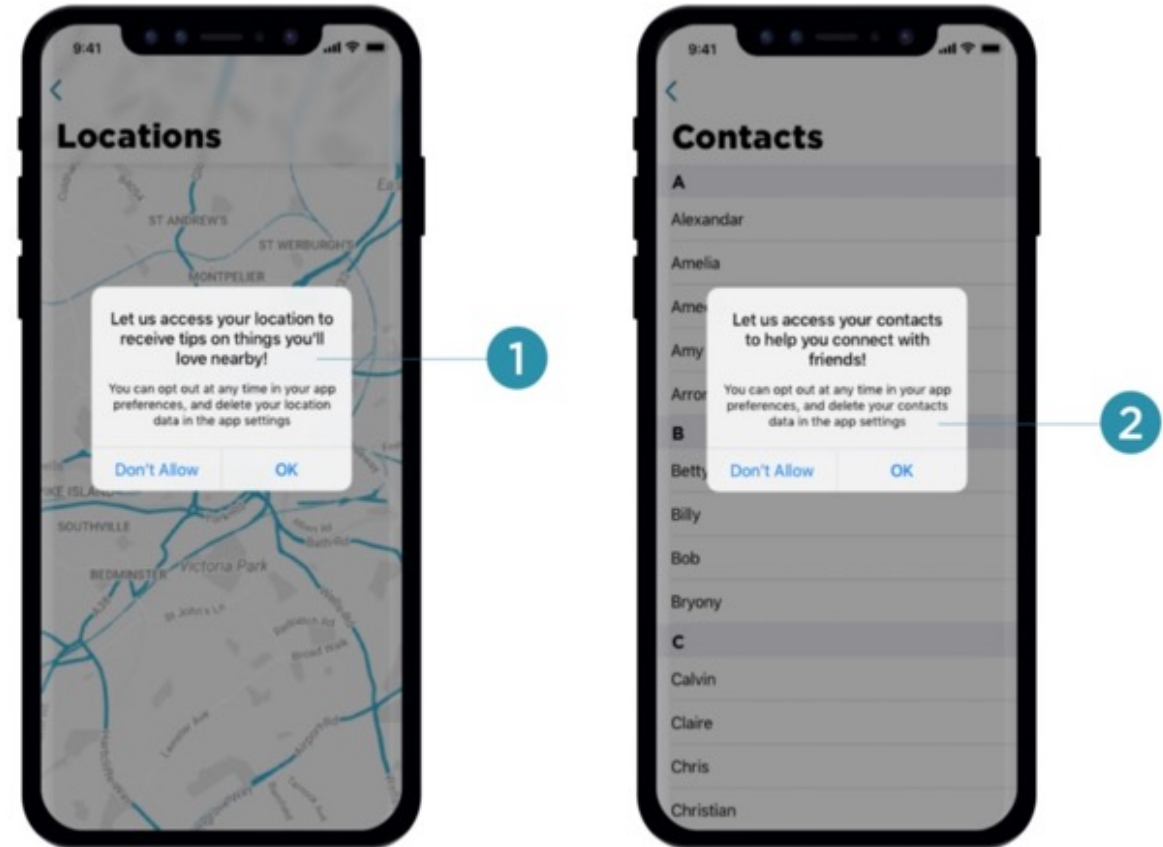
- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)



<https://fidoalliance.org/how-fido-works/>

# PETs

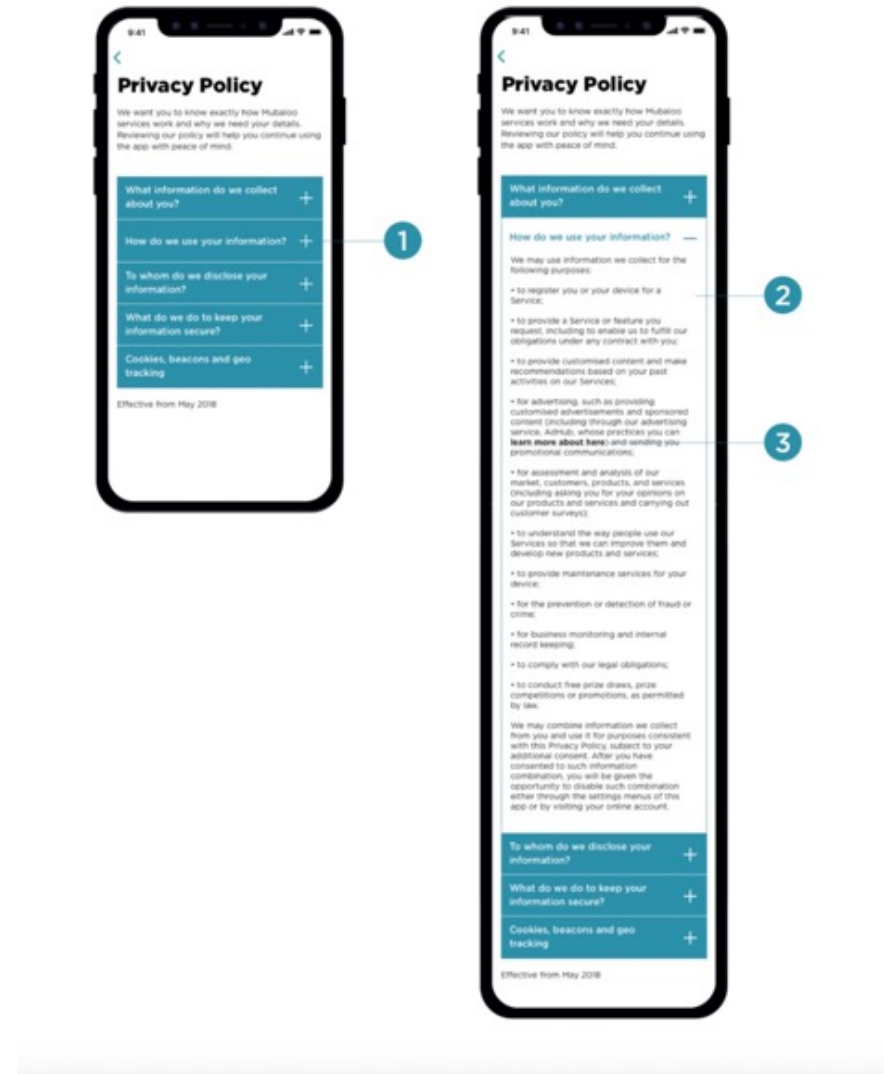
- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)
- The UX: “Just in Time” notifications



Source: Mubaloo GDPR framework

# PETs

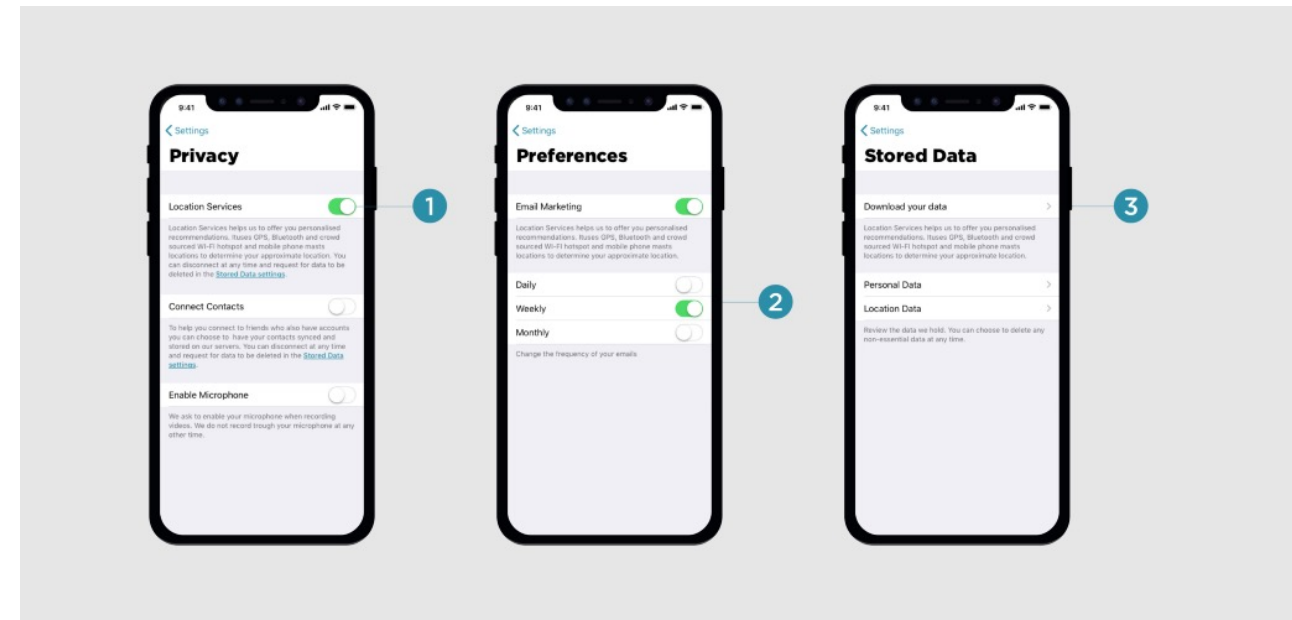
- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)
- The UX: “Just in Time” notifications, layered privacy policy



Source: Mubaloo GDPR framework

# PETs

- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)
- The UX: “Just in Time” notifications, layered privacy policy, user control



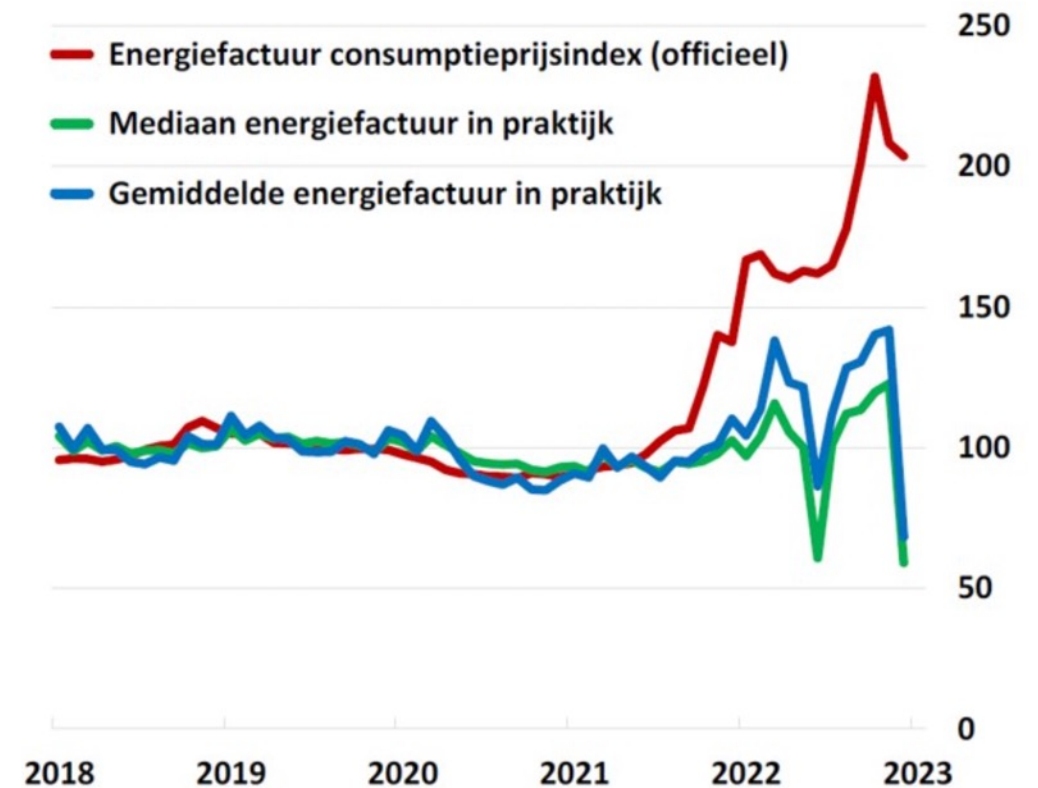
Source: Mubaloo GDPR framework

# Cases: BNP - UGent

Objective: investigate energy spending of average households (bank, university, BE)

- Transaction data anonymized *and* remains at the bank
- Ethics board approval within university, algorithm is made at university
- Run from within bank systems, output is verified by the bank before sending.
- Output is transferred to university, statistical results

Figuur 1 – Evolutie van de energiefactuur volgens de consumptieprijsindex versus de praktijk (2018 = 100)



# Cases: Local government

Objective: use smart cameras to measure population density along the coast (Local government, COVID, BE)

- Images stored on camera for only a few milliseconds
- Afterwards immediately blur passersby irreversibly, on-device
- Processing limited: only summer months and places likely to be crowded
- Security: severely limited access to system and images.
- Deactivate non-necessary functions in firmware







# Final thoughts

- It can't *just* be about privacy.
- Long term investment, but tangible benefits
- Need to involve organizations as a whole, especially management.
- Making privacy by design the default will take some time.

# Resources

- EDPB guidance on Data Protection by Design & Default: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default\\_v2.0\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf)
- Privacy Design strategies by Jaap Henk Hoepman Little Blue book: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>
- Seven Foundational Principles: [https://iapp.org/media/pdf/resource\\_center/pbd\\_implementation\\_7found\\_principles.pdf](https://iapp.org/media/pdf/resource_center/pbd_implementation_7found_principles.pdf)
- A guide to privacy by design: [https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno\\_en.pdf](https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf)
- Privacy in the product design lifecycle: <https://ico.org.uk/for-organisations/privacy-in-the-product-design-lifecycle/>
- Datatilsynet data protection by design: <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/>