Pragmatic Online Privacy: the SftE Approach

Vitor Jesus
PrivDash / Univ of Warwick / Aston University
United Kingdom

1st Intl Workshop on
Consent Management in Online Services, Networks and Things (COnSeNT)
co-located with 6th IEEE EuroS&P
• Position paper
  • somewhat speculative, definitely incongruent
  • learning the lessons so we "don't throw the baby out with the water"

• Privacy in practice
  • the paradox, the technology, the regulations

• SftE – The Start-from-the-End Approach
  • why the focus on the point of collection?
  • the speculative part: give up. It's a lost battle.
  • Focus on (1) Conventions, (2) Revocation, (3) User-managed Traceability, (4) Middleware
thank you GDPR

• It gave me words to complain – being a "computer guy"
• it is being replicated across the world
• one of the reasons for which I am proud to be an EU citizen
• (it gave me work)
thank you GDPR

• but it came at a time where personalisation had just become feasible
• the "Data-drive Economy" found in snooping its prime case

• mobile phones with rich sensors
• big data & cloud computing: vast amounts of processing power + individual profiling

“Remember when, on the Internet, nobody knew who you were?”
Privacy Matters

• yet we already lost it
"Collection-oriented" Data Protection is not working

• The focus seems to be at the Collection point.

• Mandating "cyber security" was never going to work.

• I work in Cyber Security. There will always be breaches no matter the resources you throw at it.

• the "with Privacy-in-mind", or "with Security-in-mind" only goes to a short length.
"Collection-oriented" Data Protection is not working

- it's too late by then
- a sea of grey areas
- difficult to enforce
- impossible to understand

- disempowering, un-actionable on an individual basis

vitor jesus @vjesus · Apr 12
About the April'21, 500M #FacebookLeak:
As silly as it might sound, this brilliant one-liner may hold the future of Privacy. Nothing else seems to work, anyway.

Chris Williams @ChrisNJWilliams · Apr 3
Replying to @Liz_Shepherd
How do I change my date of birth?
There is no such thing as Forward Secrecy for PETs

• Most of the time, the debates I see is on Privacy-enhancing techniques (PETs)

• PETs inherently to ignore the idea of "Forward Secrecy"
  • Cryptography: secrets are safe even after a very long time
  • when the data is out, it is only a matter of time until islands of data get linked together
SftE – the Start-from-the-End Approach

- be pragmatic
- assume the worst
- re-empower the individual
- focus on accountability
SftE – Convention

• Accept users do not exercise informed consent on an individual basis.
• make a Take-or-Leave-It attitude inconsequential

• "standardise" notices
• punish dark patterns
Personal opinion: the right to Erasure is the single most powerful principle.

The idea is similar to "changing passwords" if there's a breach.

- make Revocation automatic – 5, 30, 90 days?
- make Erasures a one-click request – standardise interfaces
SftE – Traceability

• Once shared, personal data lives in a sea or Controllers, Jurisdictions, and "3rd Parties"

• make the concept of a Consent Receipt, or Personal Data Receipt mandatory: it's user-friendly, auditable, actionable, tool-able

• codes of conduct/practice for sharing personal data
More than Cyber Security, Privacy is an after-thought.
Most times: compliance for the sake of compliance.

Browsers and apps, and everything touching Personal Data, needs to have Privacy built-in.
Mobile permissions is a great step – but baby steps.
The browser, in particular, needs a redesign.
THOUGHTS, CRITICISMS VERY WELCOME.

VJ@VITORJESUS.com

THIS IS WORK-IN-PROGRESS...