Privacy-by-Design Architecture

An operational framework

Prashant, Anubhutie, Malavika, Subodh, Subhashis

Necessary (also sufficient?) conditions for privacy

Impossibility of absolute privacy suggests that *all illegal data accesses and processing must be prevented in the first place*. (**Access control, remote execution, online regulators**)

Necessary (also sufficient?) conditions for privacy

Impossibility of absolute privacy suggests that *all illegal data accesses and processing must be prevented in the first place*. (**Access control, remote execution, online regulators**)

Data controllers must declare purpose upfront and mechanisms should exist to only allow computations that fulfil the stated purpose. (**Pre-audited, untamperable executables and data-types; regulatory boundary must extend to edge devices**)

Necessary (also sufficient?) conditions for privacy

Impossibility of absolute privacy suggests that *all illegal data accesses and processing must be prevented in the first place*. (**Access control, remote execution, online regulators**)

Data controllers must declare purpose upfront and mechanisms should exist to only allow computations that fulfil the stated purpose. (**Pre-audited, untamperable executables and data-types; regulatory boundary must extend to edge devices**)

Legitimate purpose depends on dynamically changing consent, approvals, authentication, etc. (**Consent and approval architecture**)

Necessary (also sufficient?) conditions for privacy

Impossibility of absolute privacy suggests that *all illegal data accesses and processing must be prevented in the first place*. (**Access control, remote execution, online regulators**)

Data controllers must declare purpose upfront and mechanisms should exist to only allow computations that fulfil the stated purpose. (**Pre-audited, untamperable executables and data-types; regulatory boundary must extend to edge devices**)

Legitimate purpose depends on dynamically changing consent, approvals, authentication, etc. (**Consent and approval architecture**)

Also, data minimisation should be followed as a further defence and whenever data exits the regulatory boundary (**Data minimisation as demanded by use-cases**)

Messaging

- For CS researchers: Think of privacy not in terms of crypto, SGX, encryption…, but in terms of Puttaswamy-I, Warren & Brandeis, Solove. Think architecturally and fill the gaps.

Messaging

- For CS researchers: Think of privacy not in terms of crypto, SGX, encryption…, but in terms of Puttaswamy-I, Warren & Brandeis, Solove. Think architecturally and fill the gaps.

- For CS Developers: All of the above, and that phrases like `best encryption', `industry best-practices', `data is safe', `unhackable', `100% secure', `PbD' etc. have no meaning. They should and do erode confidence!

Messaging

- For CS researchers: Think of privacy not in terms of crypto, SGX, encryption…, but in terms of Puttaswamy-I, Warren & Brandeis, Solove. Think architecturally and fill the gaps.

- For CS Developers: All of the above, and that phrases like `best encryption', `industry best-practices', `data is safe', `unhackable', `100% secure', `PbD' etc. have no meaning. They should and do erode confidence!

- For policy and legal folks: We need operational standards against which public services must hold up to. Proportionality analysis - especially the balancing part - can never be definite without such standards.