USER-CENTRIC SECURITY AND PRIVACY TOOLS

TRUST aWARE

Practical guidelines for stakeholders developing and promoting user-centric S&P tools

1. ADDRESS IMPACTS OF S&P TOOLS

Digital tools to promote S&P give rise themselves to potential S&P and other legal and ethical concerns that should be addressed.

2. MONITOR IMPACTS

Monitor impact throughout the R&D process and iterate when the S&P tool has adverse effects.

3. PROMOTE COLLABORATION

A holistic, interdisciplinary, and collaborative approach should be taken to research and development with regards to user-centric tools that promote user S&P.

4. ENSURE LEGAL COMPLIANCE

Strike a balance between protecting personal data based on its sensitivity whilst also harnessing data where it proves useful.

5. BE SENSITIVE TO DIVERSITY

When seeking to enhance privacy through S&P tools, privacy should be understood in a context dependent way which balances the needs of different individuals and is sensitive to cultural, ethnic, and socio-economic differences.

6. INVOLVE END-USERS

To ensure usability and develop user-centric tools, end-users must be involved throughout the design, development, and deployment process. Developing tools which end-users actually want should be prioritised.

7. ADDRESS THE DIGITAL DIVIDE

S&P tools should be developed and promoted in a way that helps to bridge the digital divide, particularly catering to those that need them the most during both development and deployment.

8. BE UNDERSTANDABLE AND ACCESSIBLE

When providing S&P advice, guidance, or alerting users about S&P threats, this information must be provided and explained in a transparent, understandable, and accessible manner that holds those providing that information to account.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement 101021377. The material presented and views expressed here are the responsibility of the author(s) only. The EU Commission has no responsibility for any use made of the information set out.

Read more at trustaware.eu