Prof. Carmela Troncoso
Tenure Track Assistant Professor
Security and Privacy Engineering Lab
EPFL

Towards a privacy-preserving digital society

Our digital traces have become a rich source of information about us and our environment. Increasingly, this loss of privacy results in harms for people and society. Yet, how to design and deploy privacy-preserving systems is not well-understood. Carmela Troncoso's research aims to develop technology to build digital systems that can be used without fear that the resulting digital traces can be used in harmful ways.

To achieve this goal, Troncoso and her team develop tools that support software engineers in developing complex systems in a privacy-preserving way. For instance, cryptographic techniques that enable journalists to digitally share relevant documents for their investigations without endangering themselves or their sources; mechanisms to notify those who have been close to a COVID-infected person without revealing any identities or behaviors to any third party; and protocols to enable NGOs to use biometrics without causing harms to the people they aim to help.

To complement the design activities, Troncoso's team also designs tools that help engineers to evaluate the effectiveness of privacy-preserving mechanisms to prevent information leaks. Among others, they have demonstrated that recently-proposed privacy-preserving network protocols, such as encrypted DNS, are far from sufficient to protect the privacy of users; and that synthetic data cannot be used to unleash the power of machine learning without privacy risks for users.