Selected standards for securing data sharing from ISO/IEC JTC 1 SC 27

Dan Bogdanov, PhD

Head of the Department of Privacy Technologies

About the standards committee

- ISO/IEC Joint Technical Committee 1 is an international standards organisation for information technology
- Its Subcommittee 27 works on Information Security Technologies
- Working Group 2 focuses on cryptography
- Working Group 5 focuses on identity and privacy

ISO/IEC 29100:2011 – Privacy Framework

- ISO/IEC 29100:2011 provides a privacy framework which
  - specifies a common privacy terminology;
  - defines the actors and their roles in processing personally identifiable information (PII);
  - describes privacy safeguarding considerations;
  - and provides references to known privacy principles for information technology.

ISO/IEC 29101:2013 – Privacy Architecture Framework

- ISO/IEC 29101:2013 defines a privacy architecture framework that specifies
  - concerns for information and communication technology (ICT) systems that process personally identifiable information (PII);
  - lists components for the implementation of such systems;
  - And provides architectural views contextualizing these components.

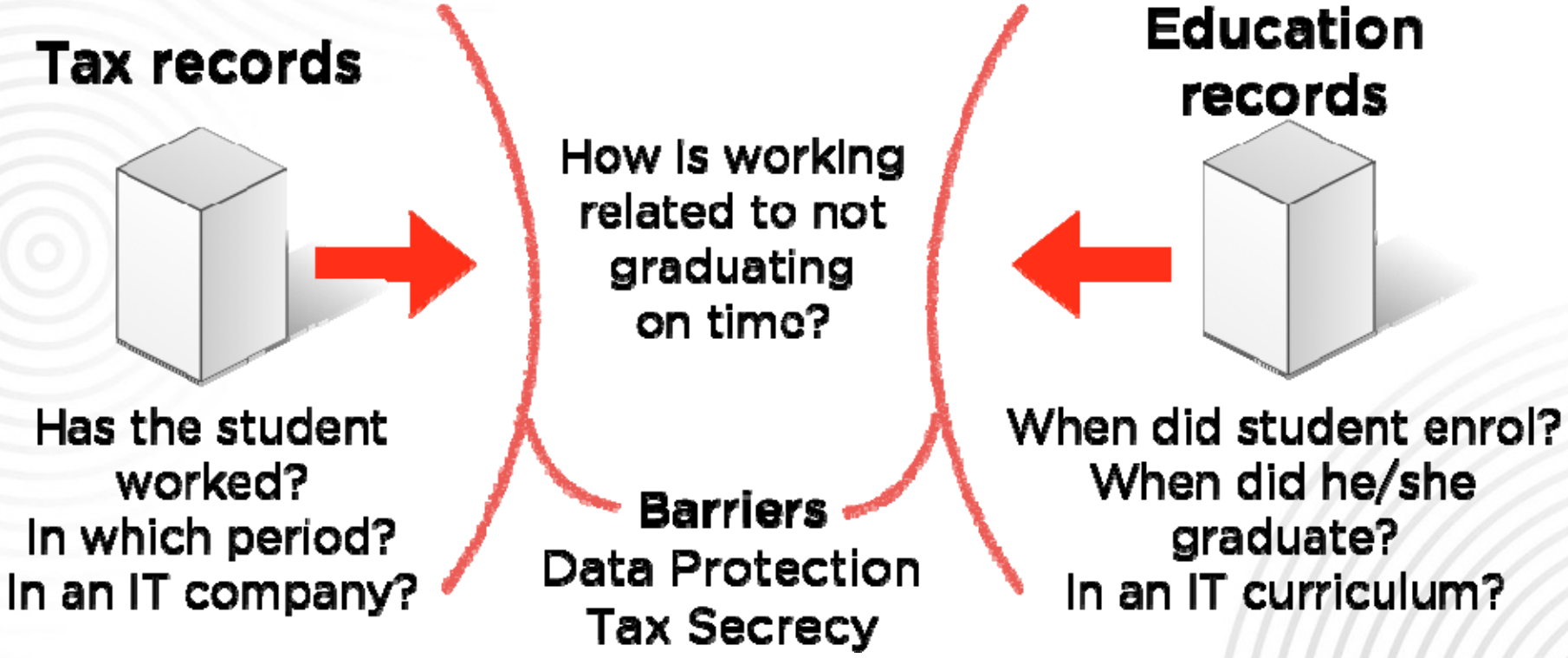
ISO/IEC 20889 – Privacy enhancing data de-identification techniques

- **NB! Under development!**
- Discusses privacy models for use in data disclosure, aggregation, statistical use.
- Describes de-identification techniques like
  - differential privacy,
  - anonymisation,
  - various kinds of encryption,
  - secret sharing.

ISO/IEC 19592 – Secret Sharing

- ISO/IEC 19592-1:2016 – Part 1: General
  - specifies cryptographic secret sharing schemes and their properties. This document defines the parties involved in a secret sharing scheme, the terminology used in the context of secret sharing schemes, the parameters and the properties of such a scheme.
- ISO/IEC 19592-2:2017 – Part 2: Fundamental mechanisms
  - specifies various cryptographic secret sharing schemes.

Example of a study using secret sharing



Key observations from the case study

- Data was collected using Secret Sharing.
- No single host/party could see any input values
- Data Protection Agency stated that data were de-identified well enough that no Personally Identifiable Information was processed in the study.
  - Thus, data protection regulation did not apply.
  - Condition: all outputs were statistical aggregates.
  - Precedent will hold under the European General Data Protection Regulation
- In-depth report of the study and comparison with *k*-anonymisation
  - Published: http://dx.doi.org/10.1515/popets-2016-0019


CYBERNETICA


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 _