

31
st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Adding Privacy To Biometric Databases:

The Setbase Approach

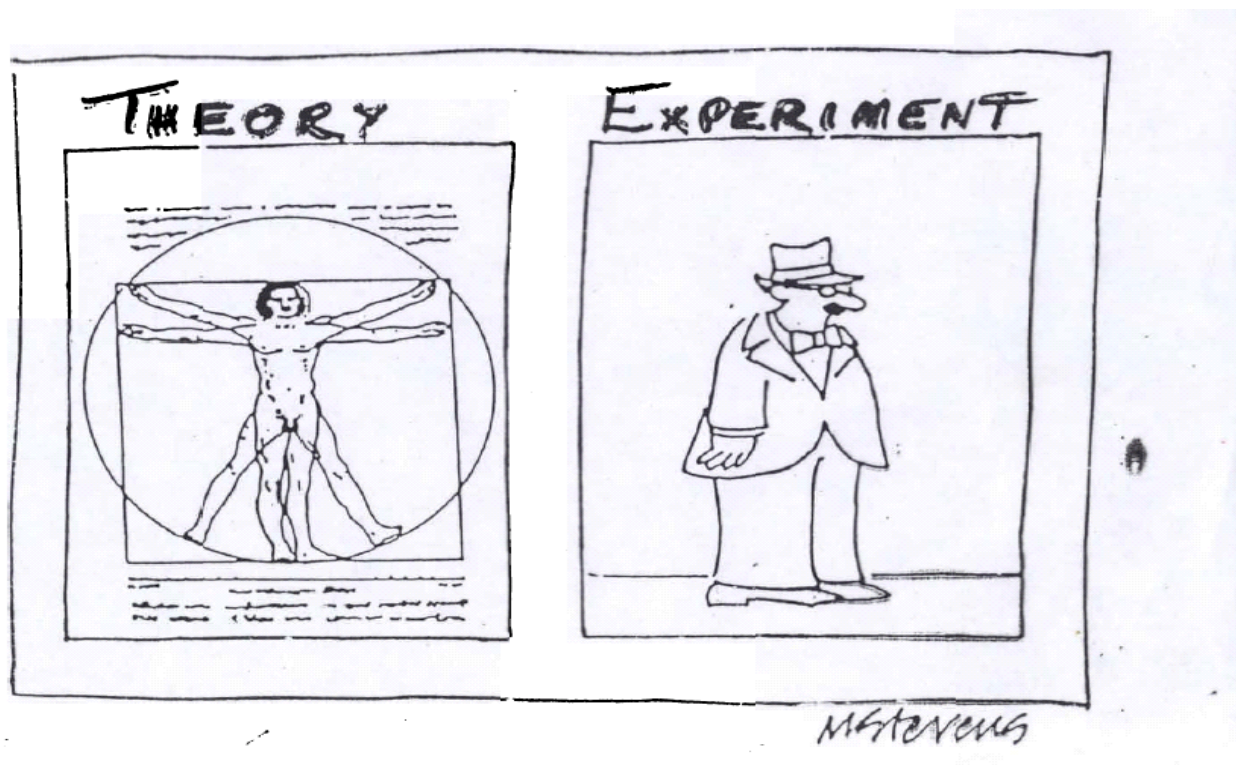
Adi Shamir
Computer Science Dept
The Weizmann Institute
Israel



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Difference Between Theory and Practice in Privacy Mechanisms of ID Cards:



- In the US: Drivers' licenses are de-facto biometric ID cards
- The FBI is not allowed by law to keep a universal biometric database, but has free access to the DMV biometric data...



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Problem: Identifying People

- Many governments (including in Israel) plan to issue new ID cards in the near future
- They are facing strong public opposition mainly due to privacy concerns
- The five possible solutions:

No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	---------------------------	------------------------------	--------------------------------	------------------------------



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Planned Transition in Israel

No universal ID card		Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	--	------------------------------	--------------------------------	------------------------------

No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	---------------------------	------------------------------	--------------------------------	------------------------------



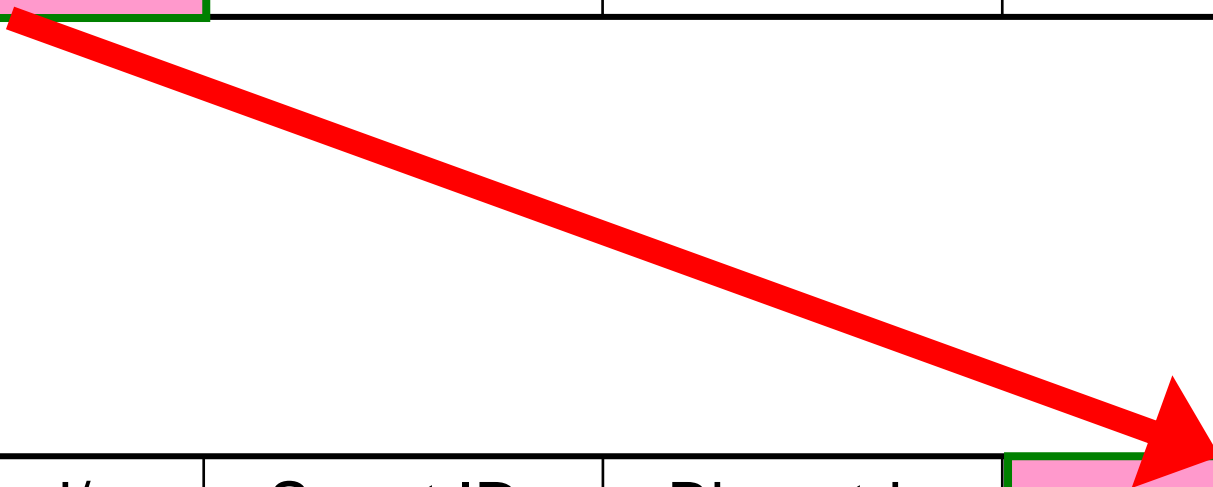
31st

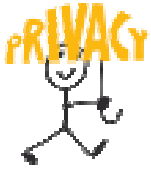
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Planned Transition in Israel

No universal ID card		Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	--	------------------------------	--------------------------------	------------------------------

No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics	Biometric ID card, no database	
----------------------	---------------------------	------------------------------	--------------------------------	--





31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Planned Transition in Israel

No universal ID card		Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	--	------------------------------	--------------------------------	------------------------------

preferred by authorities,
strongly opposed by public

No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics	Biometric ID card, no database	
----------------------	---------------------------	------------------------------	--------------------------------	--

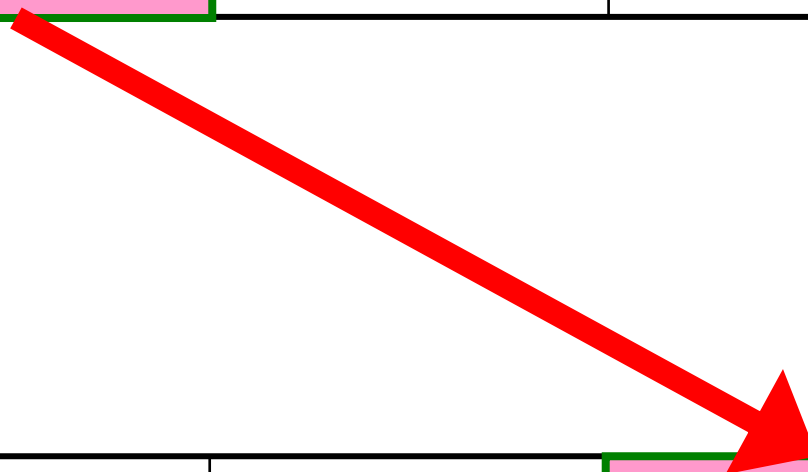


31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Planned Transition in Israel

No universal ID card		Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	--	------------------------------	--------------------------------	------------------------------



No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics		Biometric ID card + database
----------------------	---------------------------	------------------------------	--	------------------------------



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Planned Transition in Israel

No universal ID card		Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	--	------------------------------	--------------------------------	------------------------------

rejected by authorities,
almost no public opposition

No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics		Biometric ID card + database
----------------------	---------------------------	------------------------------	--	------------------------------

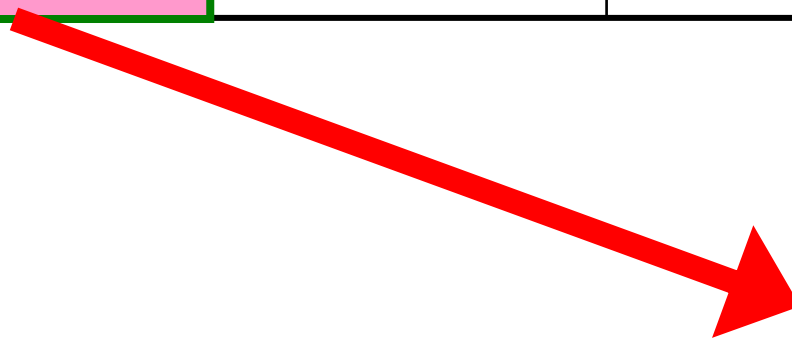


31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

My Proposal: A Biometric Setbase

No universal ID card		Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	--	------------------------------	--------------------------------	------------------------------



Biometric ID card + setbase

No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	---------------------------	------------------------------	--------------------------------	------------------------------



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

My Proposal: A Biometric Setbase

No universal ID card		Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	--	------------------------------	--------------------------------	------------------------------

acceptable to authorities,
solves most privacy concerns

Biometric ID card + setbase

No universal ID card	Printed/laminated ID card	Smart ID card, no biometrics	Biometric ID card, no database	Biometric ID card + database
----------------------	---------------------------	------------------------------	--------------------------------	------------------------------



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Official Reasons for Creating a Biometric Database in Israel:

- Major reason: Preventing double issuing of official ID cards to criminals and crooks
- Minor reason: Identifying paperless bodies and solving major crimes – in very rare cases



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Main Counterarguments of Privacy Advocates:

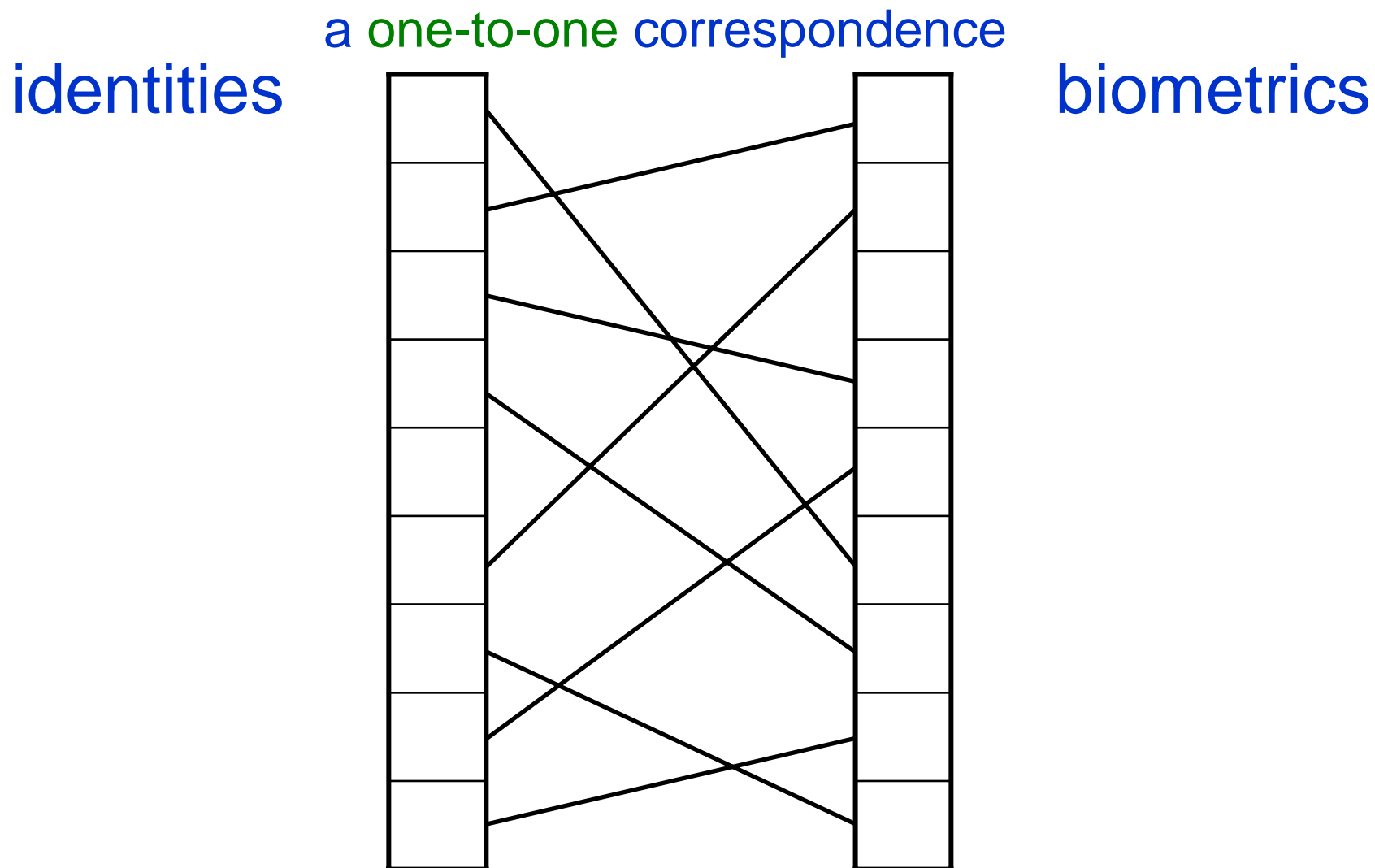
- Irreversibility: After the biometrics are collected for one purpose, there will be mission creep
- Mistrust of government: Legal protections are insufficient to prevent possible future misuse
- Insufficiency of Cryptographic Protection: Future governments can force the disclosure of keys
- Potential dangers: identifying troublemakers, entrapping innocents, leakage to outside entities

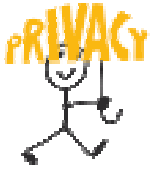


31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

A Standard Biometric Database:





31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

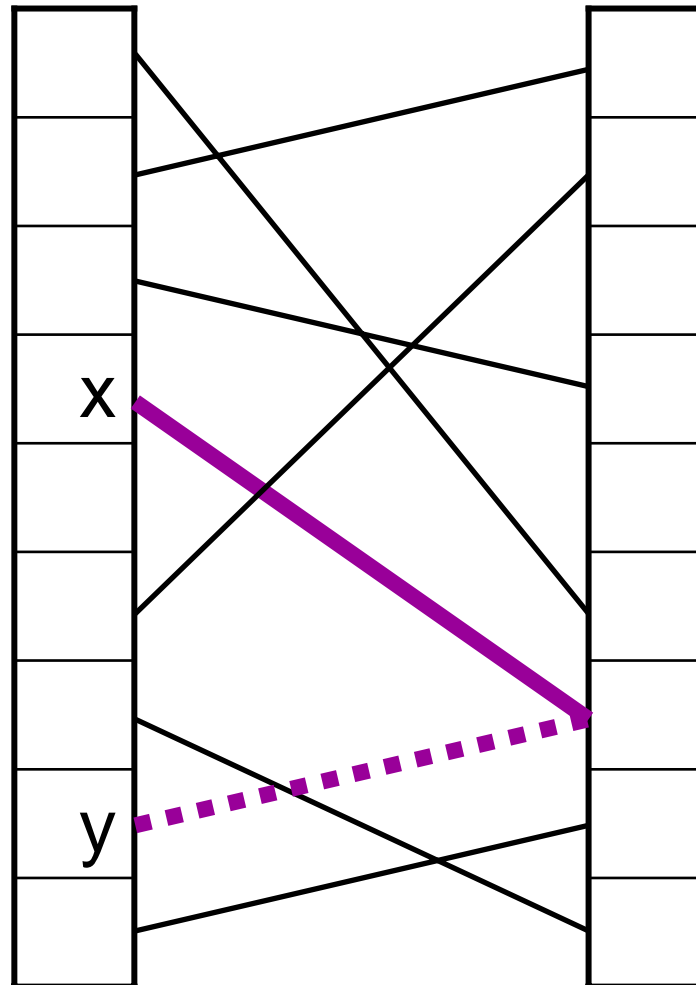
A Standard Biometric Database:

a one-to-one correspondence

identities

biometrics

when someone
who is already
registered as Mr X
claims to be Mr Y,
he will be caught
via his biometrics





31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

The Main Observation Behind Setbases:

- The database should have:
 - insufficient information to identify a person via his biometrics as Mr X
 - sufficient information to disprove a wrong claim that he is Mr Y
- This separation should remain true even if:
 - the law changes after the database is set up
 - everyone colludes with the government

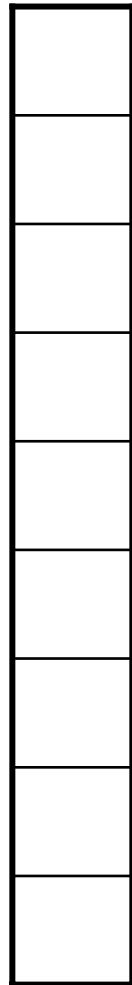


31st

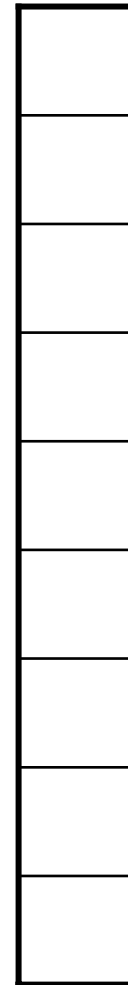
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases:

file cabinet with
all the identities



file cabinet with
all the biometrics





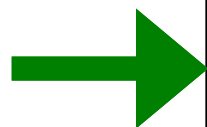
31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

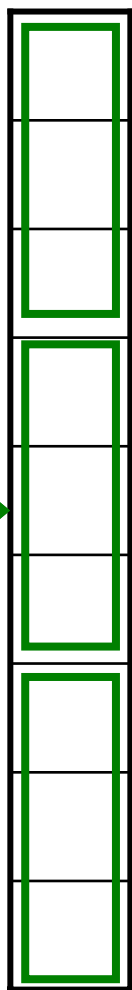
Using Setbases Instead of Databases:

file cabinet with
all the identities

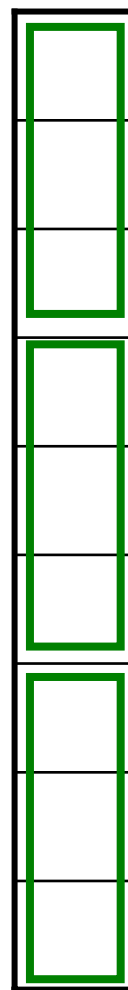
secretly and
randomly



partitioned into
drawers with
about 1,000 files
in each drawer



file cabinet with
all the biometrics





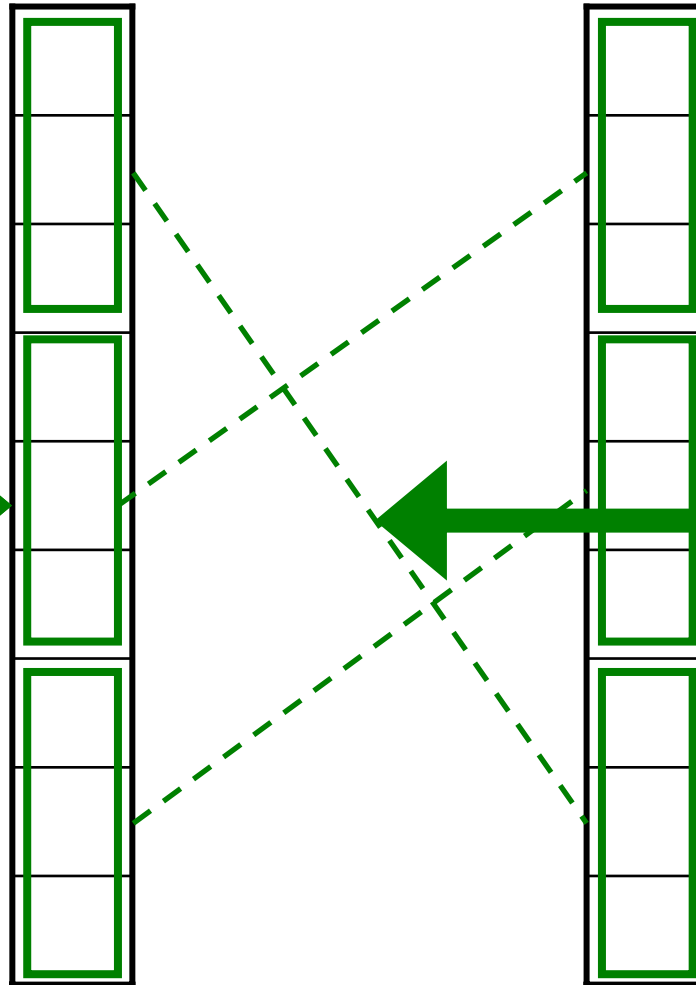
31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases:

file cabinet with
all the identities

secretly and
randomly
partitioned into
drawers with
about 1,000 files
in each drawer



file cabinet with
all the biometrics

with secret
linking
between
the drawers,
but not
between files

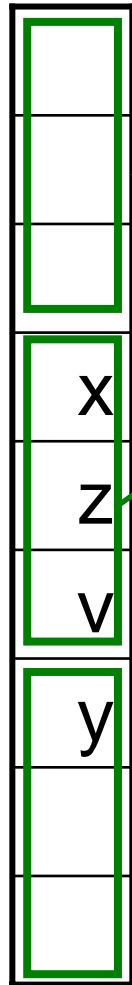


31st

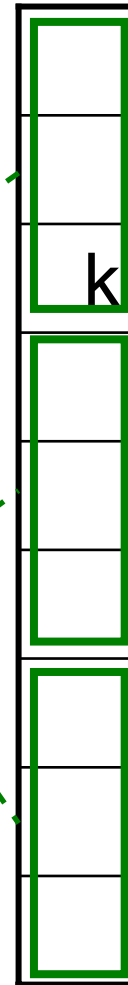
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases: How to catch cheaters

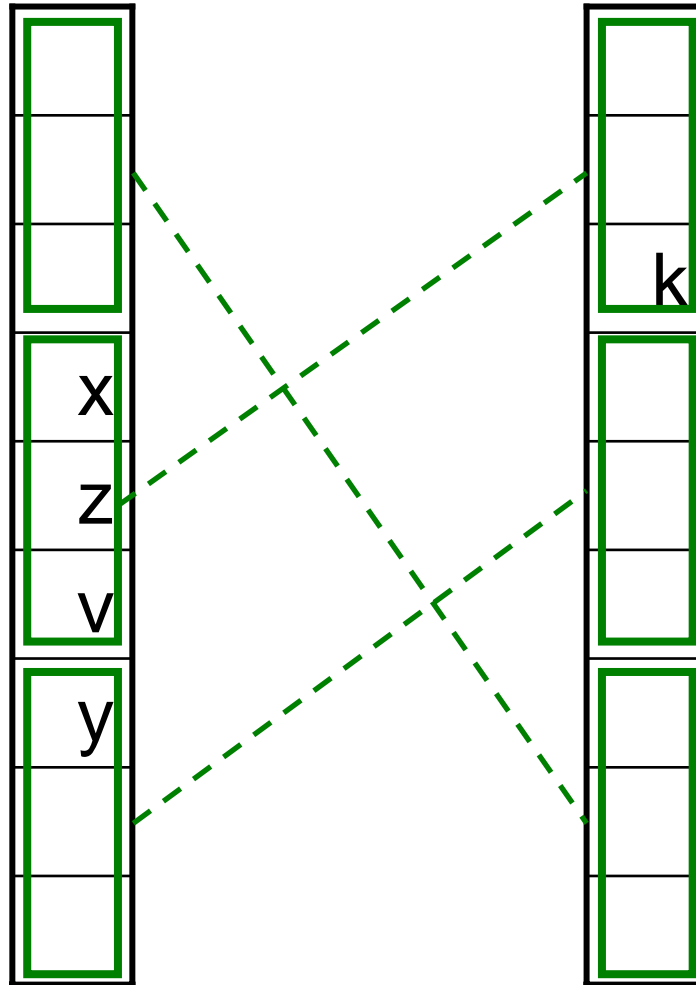
identities



biometrics



a given
biometrics
(originally
registered
as Mr x)





31st

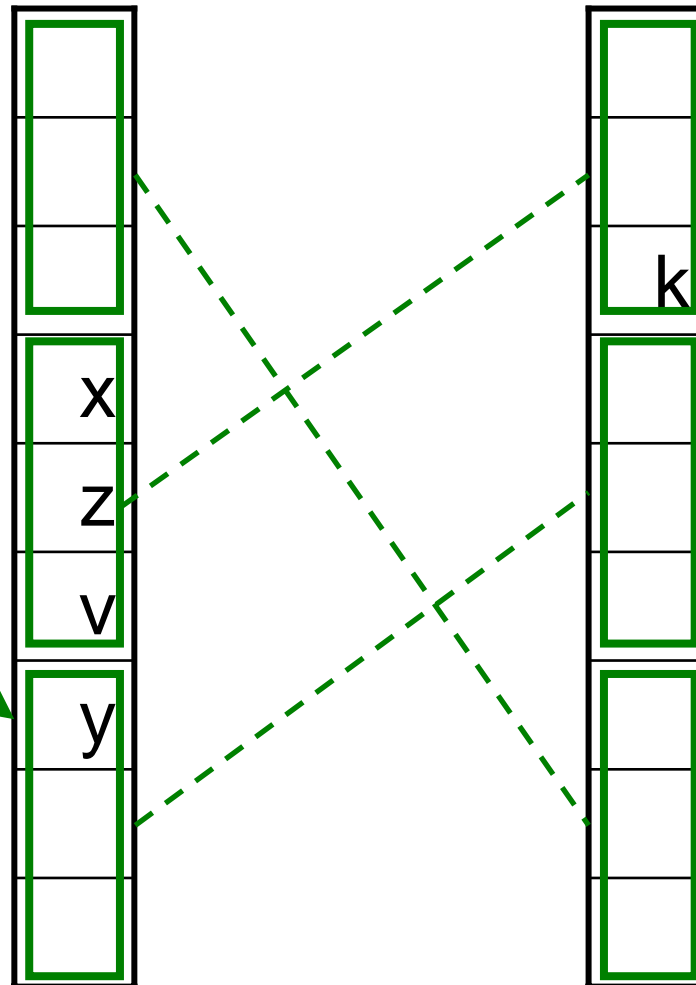
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases: How to catch cheaters

identities

biometrics

new claimed
identity y is
very unlikely
to be in the
same secret
subset with
the original x



a given
biometrics
(originally
registered
as Mr x)

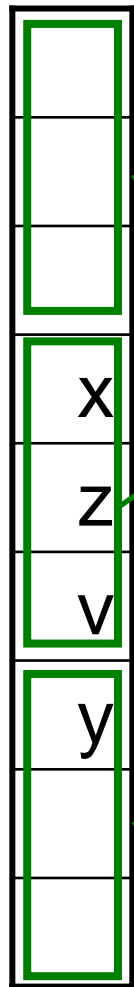


31st

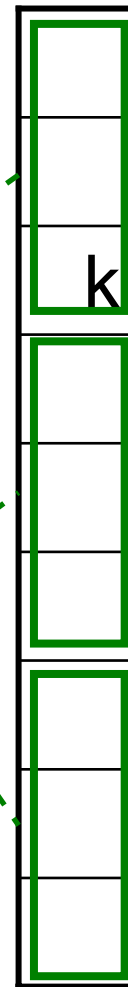
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases: How to Identify Paperless Bodies

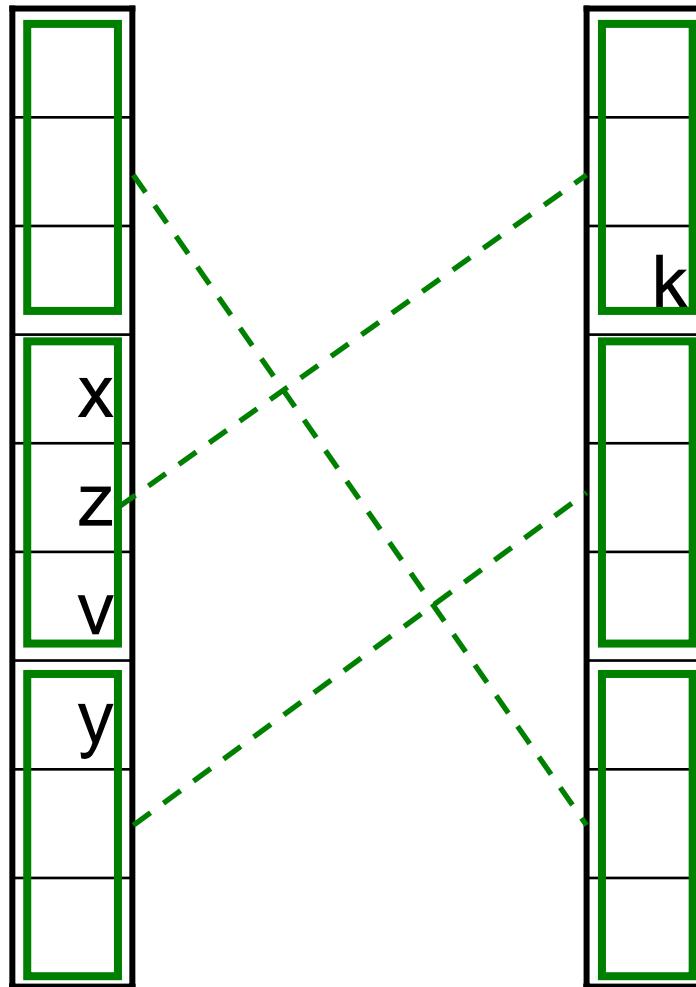
identities



biometrics



a given
biometrics
(originally
registered
as Mr x)





31st

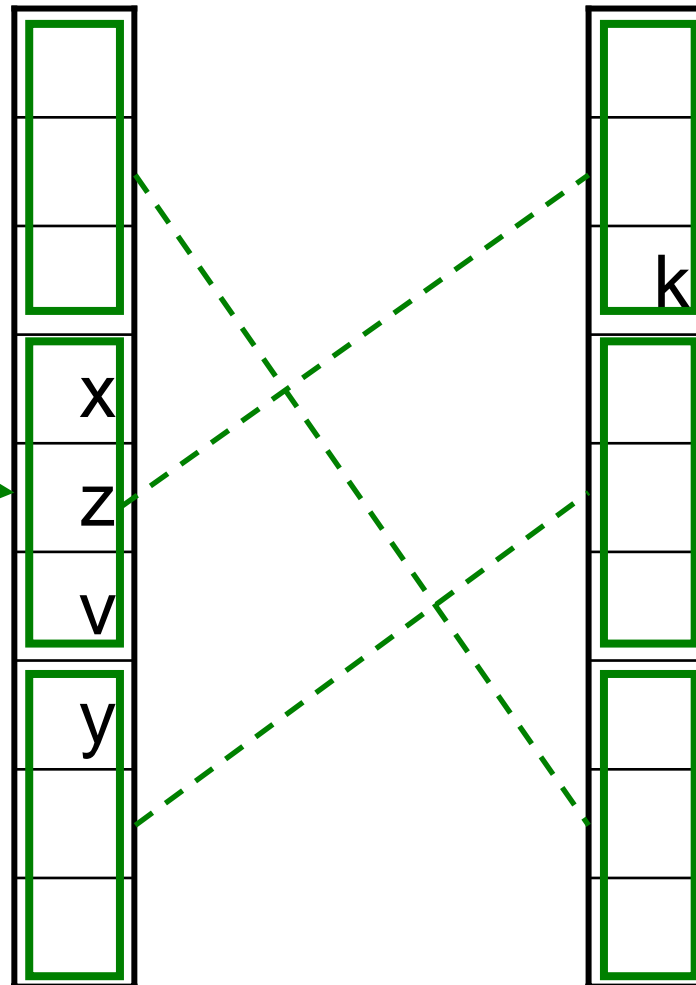
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases: How to Identify Paperless Bodies

identities

biometrics

Police will investigate all the 1000 linked identities, reduced to 100 By gender, age, etc



a given biometrics (originally registered as Mr x)



31st

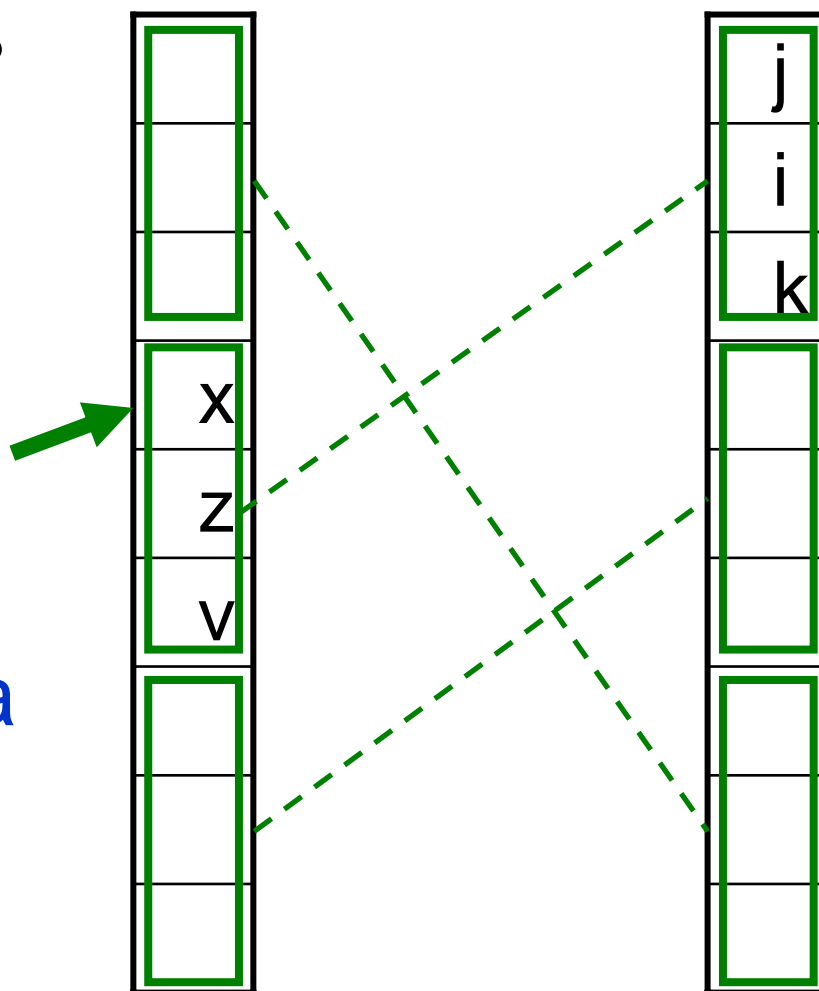
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases: Even Fully Leaked Data Cannot Entrap

identities

biometrics

someone with full access to the data wants to **entrap x** by planting his fingerprints in a crime scene





31st

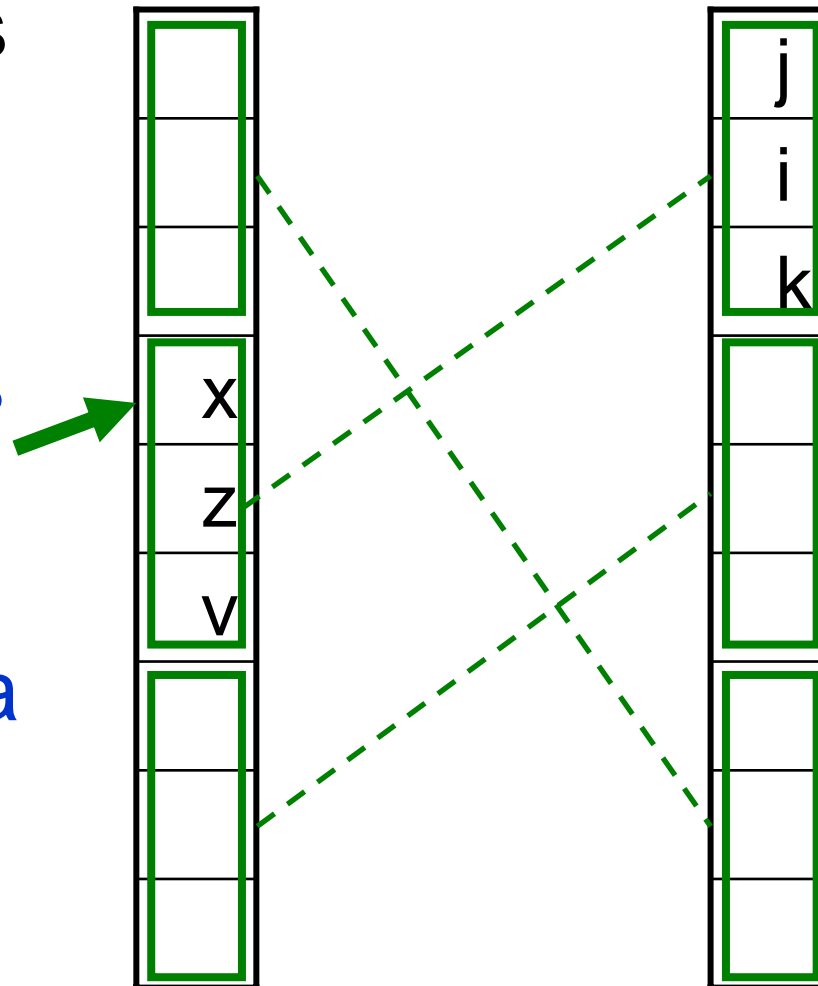
Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Using Setbases Instead of Databases: Even Fully Leaked Data Cannot Entrap

identities

biometrics

someone with full access to the data wants to **entrap x** by planting his fingerprints in a crime scene



planting one fingerprint has **probability of 1/1000** to succeed; planting multiple fingerprints will **raise alarm**



31st

Madrid, 4th, 5th and 6th, November 2009
international conference
of data protection
and privacy commissioners

Summary:

- Like any other privacy enhancing technique, setbases are a compromise between the conflicting demands for privacy and functionality
- Double issuing can be prevented at almost no additional cost and with very high probability
- Individuals can be identified from their biometrics, but only by a long, expensive and highly visible police investigation, and can't be easily entrapped
- This privacy protection cannot be eliminated by changing the law or expropriating the crypto keys