

Biometric ID: Robust Enough for Development?

TABULA RASA Workshop

Peter Went, CEO



Rome
May 10th, 2012

Points for Debate

Alan, slide 10: If ID is essential for rights, then cost cannot be a barrier



Alan, slide 12: Much wastage of resources on transient, single-purpose identification programs/components



Alan, slide 22: UK: card security reported vulnerable; US concern over BELIEVE Card. Card security one reason UID chose a central database



Peter: Identity is a right (to get benefits) and an obligation (to be traceable)



Peter: Strong identity (accuracy at scale & inclusion) over Weak identity (ease)



Question: Spoofing accepted (impersonation) or Strongest identity (including Time & Location: Minority Report, Orwell)



What if I had no Identity?

❖ I can not own property

- Because you need to identify yourselves to buy it
- And you need to be able to prove you own it
- And to identify you when you want to sell it

❖ I can not open a bank account

- Because I need to identify myself

❖ I can not earn money

- Because an employer needs to certify the true identity of a person

❖ I can not register myself as a citizen

- Because I need to identify myself
- And show breeder documents, which I do not have because I don't have an identity

❖ I can not vote

- Because every voter needs to prove their identity prior to voting

❖ I can not get unemployment benefits

- Because I need to have worked in the first place, which I cannot
- And I need to have a bank account to receive payments
- And I need to identify myself as registered in The Netherlands
- And prove my identity

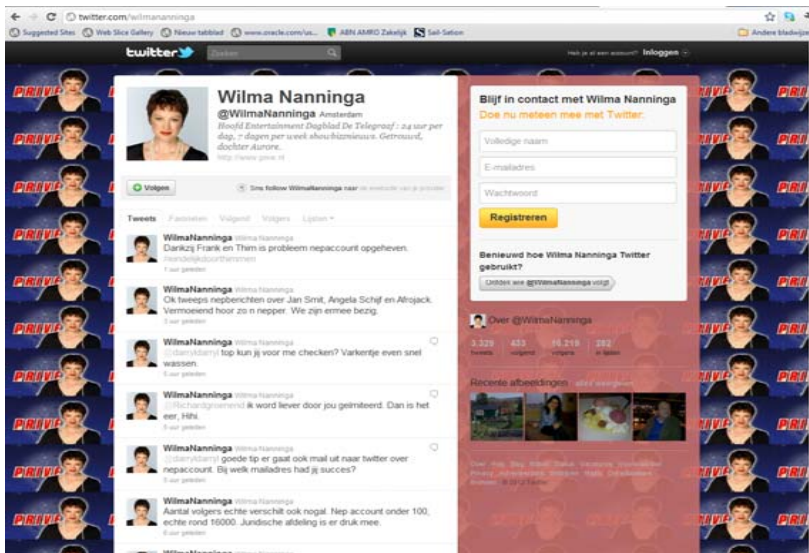
Point being

➤ *I cannot survive without a credible identity*

What if I had a Weak Identity

❖ Impersonator: “trying to assume the identity of another”

- *Wikipedia: An **Impersonator** is someone who imitates or copies the behavior or actions of another, possibly as part of a criminal act such as identity theft. This is usually where the criminal is trying to assume the identity of another, in order to commit fraud, such as accessing confidential information, or to gain property not belonging to them. Also known as social engineering and impostors..*



Impersonation is easy:

- *To get an email address, URL, Twitter account, LinkedIn page, Facebook page, Skype account that resembles someone's name is as easy as 123*
- *The truth is in the eyes of the beholder. So if people believe it is real, they will act on it as if it were real*

Point being

- *Spreading chaos or causing damage is easy*
- *Strong(er) identification is required*

Strong Identity over Weak Identity

- ❖ **Identification:** “entities are the same if they have all their properties in common”
 - *WIKIPEDIA: The **identity of indiscernibles** is an ontological principle which states that two or more objects or entities are identical (are one and the same entity) if they have all their properties in common. That is, entities *x* and *y* are identical if any predicate possessed by *x* is also possessed by *y* and vice versa. A related principle is the indiscernibility of identicals, discussed below.*
- ❖ **Single Modal:** “an object or entity is identified by one property”
 - *That means many objects or entities will be considered the same quite easily*
 - *That means identity theft, deliberate or not, is relatively easy*
- ❖ **Multi Modal:** “an object or entity is identified by a combination of many properties”
 - *That means one has to disclose a lot of information about him or her self*
 - *That means identity theft, deliberate or not, is complex*



More is better, but:

- More modalities make a stronger identification
- **But, it flips the ‘Innocent until proven guilty’ coin**

Point being

- Strong identification is inevitable
- But let’s focus on possible implications

Spoofing vs Strong(est) Identity

❖ Spoofing: “forging a modality”

- It is always possible to spoof
- Certain modalities are easier to spoof than others
- Spoofing many modalities is more difficult than spoofing a single modality, but still doable

❖ Strongest Identity: “Multi Modal + Location + Time (= Big Brother)”

- If we assume anything can be spoofed, we need to add other factors into the identification
- Adding location and time into the mix, makes it impossible to impersonate without that being noticed



Developed countries:

- Few Trxs x High Value (Assets) = High Risk
 - Many Trxs x Low Value (Internet) = High Risk
- Strong identification is required!

Developing countries:

- Many Trxs x Low Value (Rural) = High Risk
- Strong identification is required!

Point being

We cannot escape from strong identity

Summary

- ❖ We live in a global society
- ❖ Therefore we need global identification
- ❖ Which implies scale
- ❖ That requires strong(est) identity
- ❖ For accurate identification of anybody (inclusion)
- ❖ Preventing impersonation and spoofing
- ❖ Resulting in a trusting society

In a Global Society:

Weak identity → Spoofing & Impersonation

Strong(est) identity → Anti-Spoofing & Trusted Identity

and what is your opinion?

- Point 1 (Alan):* If ID is essential for rights, then cost cannot be a barrier
- Point 2 (Alan):* Much wastage of resources on transient, single-purpose identification programs/components
- Point 3 (Alan):* UK: card security reported vulnerable; US concern over BELIEVE Card. Card security one reason UID chose a central database
- Point 4 (Peter):* Identity is a right (to get benefits) and an obligation (to be traceable)
- Point 5 (Peter):* Strong identity (accuracy at scale & inclusion) over Weak identity (ease)
- Point 6 (Question)* Spoofing accepted (impersonation) or Strongest identity (including Time & Location: Minority Report, Orwell)

WCC Smart Search & Match

WCC Smart Search & Match:

- A platform for multi-modal fusion
- Extremely fast, scalable and accurate
- Matches on biometric & biographic data

For more information:

Peter Went

PWent@WCC-Group.com

WCC Services B.V.
Savannahweg 17
3542 AW Utrecht
The Netherlands

WCC Services, Inc.
Two Fountain Square
11921 Freedom Drive
Suite 550
Reston, VA 20190

