MULTIMEDIA TRAINING KIT

Case studies: The right to privacy

Developed by: Carly Nyst

Case studies for discussion

India's unique identity scheme

Since 2009, the Indian government has been putting in place a plan to record the unique biometric identity (UID) of the country's 1.2 billion citizens. The UID connects personal information with biometric data such as fingerprints and retina scans, making every Indian individually identifiable.

The Indian government believes that the UID will help to make every citizen, particularly the poor and marginalised, visible, giving them legal identity. The UID will become the way that the poor can access government services and benefits, and will help to wipe out corruption. Delivering public services to a population of over a billion people is an impossible task unless the government is able to identify and reach everyone one of those people. The UID will be a huge advancement in this respect.

Critics of the UID system say that rather than becoming a means of inclusion, the UID will have an exclusionary effect. Even though the UID is ostensibly a voluntary initiative, many Indian government departments are already demanding a UID before enrolling an individual in a service. Banks may also make a UID a prerequisite for opening or maintaining an account. Indians require the correct documents to enrol in the scheme; unfortunately, many of the poorest and most marginalised do not have such documents. The poor face other barriers: the requirement that they have a fixed address; differences in the spelling of names that have rarely been written; even the simplest problem of having hands calloused and worn by a life on the streets or in rural areas may prevent them from providing fingerprint data. There is already a considerable amount of debate as to the reliability of biometrics; the US National Research Council concluded in September 2010 that the current state of biometrics is "inherently fallible".

There are also concerns about data security, given the many places that data reside during the establishment of the UID system before they reach the Central Identities Data Repository. Once they reach the central database, concerns turn to the use of the data to surveil and monitor the population, as the UID database is linked to the national intelligence grid. There is a concern that the state will become an all-controlling body that is able to repress social movements, political dissent or public critique under the guise of quashing corruption.

What are the implications of the UID for the right to privacy?
Where should the balance between privacy and security lie?
Is keeping track of Indian citizens and providing them with public services more important than respecting their privacy rights?

Mining consumer data

As part of improving customers' experiences and seeking to offer them more efficient and convenient services, many retailers collect information about their customers. This can be done by connecting a customer to the credit card they use, or to a survey they fill out, a form they sign or a coupon they use. Gradually, a store could develop a complete profile on a customer, and then start marketing special offers or discounts to them in a unique way. This not only improves the retailer's sales effectiveness, but it also enables the customer to have a more personalised, relevant shopping experience.

In the US, Target – a one-stop shop for everything from homewares to groceries – established a Guest ID for each of its customers, linking credit card information with age, family status, address, salary and websites visited. Target can buy data about an individual's ethnicity, job history, the magazines they read, home ownership, education history, etc. They can then analyse that data and predict what customers might like to purchase next.

In the early 2000s, Target began analysing the shopping habits of pregnant women. Seeking to secure the women as Target shoppers before their baby was born, Target wanted to know what indicators to look for to find out if a woman was expecting, so that they could send her coupons and other shopping incentives. Using data mining, they discovered that women bought large quantities of unscented lotion around the beginning of their second trimester. In the first 20 weeks, pregnant women buy calcium, magnesium and zinc supplements. Close to their due date, they buy scent-free soap, cotton balls, hand sanitisers and washcloths.

Based on this and other information that Target had been able to derive from the data collected, Target began analysing the shopping habits of a teenage girl, Sarah, and concluded she was pregnant. They began sending coupons to her house advertising pregnancy-related items. Her parents received the coupons and were extremely upset that Target would be encouraging their teenage daughter to get pregnant. As it turns out, the girl was pregnant, but had not told her parents. Target knew before the parents knew.

Has Sarah's privacy been violated? Why/why not?
What obligations did Target have with regards to the personal information they collected about Sarah?
What opportunity did Sarah have to control the information that Target held about her?

Real-name registration in Asia

In 2007, the internet real-name system was introduced in South Korea, requiring media sites with more than 100,000 visitors per day to record the real identities (including identity registration numbers) of visitors who have posted comments.

Proponents of the real-name system argued that it is necessary to curb a spate of cyber bullying, which had seen a number of posted comments describing fabricated sex scandals and other untrue controversies involving celebrities. Reports linked these comments to a number of suicide attempts by people who were the subject of the bullying. The real-name system was introduced to facilitate the bringing of actions for libel or infringement of privacy by the individuals being bullied.

In August 2012, the country's Constitutional Court overturned the rule, on the basis that it restricted freedom of speech and undermined democracy. The Court said that the policy discouraged free expression and open criticism of influential people and groups because of fears of punishment. It also found that the system made it easier for cyber criminals to commit identity theft.

Under new rules introduced in China in December 2012, Chinese service providers will now be required to obtain real-name information from all of their users.

Does real-name registration promote respect for the right to privacy?
Does anonymity encourage individuals to violate others' privacy?
How should the balance be struck between privacy and freedom of expression when it comes to real-name registration?