Toronto first to use biometrics for welfare benefits

The Corporation of the Municipality of Metropolitan Toronto (Metro) is on the verge of being the first government in Canada to use identification technology in the provision of welfare benefits. In June 1996, Metro Council, the governing body of the Corporation composed of elected representatives, approved use of a biometric identifier as part of a programme to enhance service delivery and strengthen the integrity of social assistance processes. Metro's Rita Reynolds reports.

The problem is fraud

A deep recession in the first half of the 1990's, resulting in ballooning caseloads and erosion of the tax base, fuelled the drive to overhaul antiquated paper-based systems and realise the benefits prudent use of technology can bring. A programme of administrative streamlining, process automation and staff training produced a leaner system but did not meet the challenge of fraud.

Under the law of the Province of Ontario, the Metro benefit system rests on two tests; identification and need. However, while we continue to rely on industrial age identifiers, technology advances and stolen identification are undermining the tests. Birth certificates, passports etc. are all inferential; the individual holding the record is presumed to be the rightful owner. Where photographs are used as an identifier, such as in driver's licenses, they can be replaced. These weaknesses in our identification systems attract the unscrupulous and undermine the security of personal information.

Governments and financial institutions are vulnerable to fraud and individuals to theft of identity because industrial age identifiers do not establish a positive link between an individual and their documentation. Since stolen or forged identification documents can open public vaults to tax-free cash they become valuable commodities, creating a black market in personal information and threatening the privacy of wholly innocent individuals. This fraud on government benefits and rights of citizenship, and the resulting invasion of personal privacy, is a growing societal concern.

Just as technology offers the means to undermine the integrity of benefit systems, it also offers the means to protect privacy and deter fraud. Biometric technologies (biometrics) record unique characteristics that may be used to distinguish an individual. Retinal scanning, voice identification, digital photographs and finger scanning are some of the biometric technologies being used to restrict access to high security facilities or speed travellers through customs and immigration checkpoints.

The solution is encrypted biometrics

The Municipality of Metropolitan Toronto is the sixth largest government in Canada and serves a population of 2.5 million. Metro's social assistance caseload ranges between 100,000 and 120,000 cases. To provide better service and counteract the incidence of stolen cheques, optional direct bank deposit was introduced, the acceptance rate is almost 70%. Remaining are thirty thousand cheques issued every month and stolen cheques, cashed with forged identities, account for an annual loss of approximately $600,000. The incidence of duplicate or multiple claims, based on false identifiers, is conservatively estimated at 3%, an annual loss of about $27.5 million.

Metro Council's decision to use an encrypted biometric was predicated on the need to staunch fraudulent cash outflow, preserve benefits for the destitute and fulfil the elected representatives' fiduciary obligation to the public. The specific biometric to be used is under consideration.

At the time an individual makes application for benefits, an electronic comparison will be made between an applicant's biometric identifier and those of current recipients, a one-to-many search. To protect privacy, encryption of the biometric and storage on a secure database separate from the textual information was made mandatory.

An encrypted biometric obtained through scanning an individual's finger patterns appears to be a privacy protective technology appropriate to a social assistance delivery system. Finger patterns are unique to each individual and a one-to-many search may be conducted with sufficient accuracy to answer the primary question: is the applicant already in receipt of benefits? Encryption at the point of collection provides anonymity and security, taking the process light years ahead of traditional forms of identification, i.e. one cannot

look at an encrypted finger pattern and recognise an individual as being in receipt of benefits.

On enrolment, social assistance clients will receive a bank card which will enable them to withdraw from any ATM the benefit to which they are entitled. Consideration was given to using a photograph on the bank card and/or an additional encrypted biometric; however, both were rejected as an unreasonable infringement of privacy as neither are required to interact with a machine and account security is maintained with a PIN.

Ontario privacy legislation requires government institutions to limit collection of personal information necessary to deliver a mandated service. Within this context, selection of a biometric is dependent on the identification function(s) performed. Legislation entitling individuals to social assistance presumes disbursement of only one benefit per person. A primary obligation is to eliminate multiple benefit payments to one individual. The function of a biometric consequently has a limited goal of determining whether or not an individual is already enrolled. The biometric identifier does not address the test of need. However, even in the case of a fraudulent claim of need, it limits the loss to one payment rather than many.

A broader role for drivers' licences

In contrast, the biometric identifier on a driver's licence fulfils a broader role. The identification function must provide for ongoing confirmation that an individual is licensed. For this reason, a photograph, ideally digital, is the biometric often used. This allows an officer who stops a driver to compare the individual to the photograph on the license, confirming they are one and the same.

Digitising the photograph, thereby enabling instantaneous comparison with the primary enrolment database containing both the license serial number and the photograph of the originally licensed individual, eliminates forgeries. The process is a one-to-one search; serial number to serial number and a photo comparison. Nothing is revealed in making the comparison that the officer cannot already see - gender, facial characteristics, race and approximate age. Confirmation that the individual is the legitimate holder does not reveal other personal data the officer does not need in the performance of his duty. In this context, a photograph meets a specific functional requirement without unnecessarily invading privacy.

Health care systems have greater privacy requirements

The identification functions in the health care system encompass those required in the social assistance and driver's license systems. In countries where the costs of health services are paid through the tax base, there is a need for both enrolment identification and ongoing verification of entitlement. While medical information is highly sensitive, knowledge that an individual possesses a health card does not give rise to the same privacy concerns as a card identifying him as being in receipt of social assistance benefits. A digital photograph on a health card provides for ongoing verification and, as with the licensing example, does not reveal information a medical practitioner does not need or does not already know.

> "Failure of public authorities to use information technology in the face of unscrupulous individuals or organisations which do, will undermine essential benefits systems and promote criminality"

Privacy enhancing technologies such as encryption allow use of biometrics to establish a secure link between individuals and their personal information. Failure of public authorities to use information technology in the face of unscrupulous individuals or organisations which do, will undermine essential benefits systems and promote criminality. Biometric identifiers are not a panacea and the design of systems must be strictly limited to meeting the identified function, but they are essential to public and private financial systems in the age of information technology.

Report by Rita Reynolds, privacy advocate, who has corporate responsibility for access and privacy legislation in the Municipality of Metropolitan Toronto. Internet address: rita_e._reynolds@metrodesk.metrotor.on.ca