

Detection, Identification, and Authentication Systems

The Challenge

Government systems for detection, identification, and authentication will often have essential national purposes to support. These purposes might be national security, enforcing national borders, enabling law enforcement, or maintaining public order. Such systems usually require the gathering of personal data about individual citizens. These data might be biometric data. They could equally be DNA, identifying data such as name and address and d.o.b., CCTV images, or internet traffic logs.

Such systems create a dilemma. Governments put these systems in place to protect their citizens. However, citizens often feel threatened by these systems more than they feel protected. Citizens will often focus on the threats to their personal interests arising from these systems more than on the threats to the society of which they are a part which these systems are intended to address. As a result, governments face a difficult challenge: maintaining the individual citizen's confidence that their personal interests are being protected whilst enabling these systems to meet the national needs for which they were developed.

Citizens' Fears and Concerns

Whilst the citizen might understand and support the purpose for which such a system has been developed (e.g. national security, law enforcement, public order), their fears and concerns are real and need to be acknowledged and accommodated if citizen confidence is to be maintained. Citizens are often concerned for their privacy. However, their fears and concerns range beyond privacy alone. Citizens are right to be concerned that their personal information could be used in ways which are contrary to any aspect of their personal interest. For example, they might fear their information being used to profile them and then to treat them in a way which they feel is unfair, such as to restrict their access to services or entitlements, or to increase the premium they pay for insurance. They might fear the information being incorrect and that they could be refused a service to which they are entitled or have paid. They might fear that the information could fall into the wrong hands and be misused, perhaps to harm them physically, for theft, or to embarrass harass or blackmail them.

Address Through Governance

These fears and concerns can be addressed without diminishing the system's ability to support the intended national purpose. The solution is to develop a suitable governance framework for the system, and to develop that framework at an early stage in the system's design.

A governance framework will acknowledge explicitly that:

- Individual citizens have legitimate interests which can be affected or harmed by the uses, proper and improper, made of their personal data;
- Government, acting on behalf of the public at large, also has legitimate interests, such as the maintenance of law and order, the maintenance of national security, the prevention, detection and investigation of crime;
- In some situations, the interests of the citizen and the interests of their government will, rightly and unavoidably, be in conflict with each other.

The objective of a governance framework is to ensure that the interests of all parties are protected in proper balance in all situations. In particular, this includes ensuring that when the legitimate interests of the individual citizen are rightly overridden in the national interest, the citizen remains adequately protected so their interests are not harmed unnecessarily or inappropriately in the process. It is through the creation of a suitable governance framework that the balance of conflicting interests can be agreed and all the relevant safeguards and protections specified.