ELECTRONIC FRONTIER FOUNDATION

Mandatory National IDs and Biometric Databases

Mandatory National IDs and Biometric Databases

Mandatory nationwide identification systems have been implemented in a number of countries including Argentina, Belgium, Colombia, Germany, Italy, Peru, and Spain. While these schemes vary by country, individuals are typically assigned an ID number, which is used for a broad range of identification purposes. Large amounts of personal data such as name, birth date, place of birth, gender, eye color, height, current address, photograph, and other information is linked to this ID number and stored in a centralized database. In many countries, such as Argentina, national ID regimes are adopted during military or authoritarian regimes.

National ID cards and the databases behind them comprise the cornerstone of government surveillance systems that creates risks to privacy and anonymity. The requirement to produce

identity cards on demand habituates citizens into participating in their own surveillance and social control.

Biometric Identifiers in a National ID Scheme

Many countries are now "modernizing" their ID databases to include biometric identifiers that authenticate or verify identity based on physical characteristics such as fingerprints, iris, face and palm prints, gait, voice and DNA. While supporters argue that biometric identifiers are an efficient way to accurately identify people, biometrics are costly, prone to error, and present extreme risks to privacy and individual freedom.

Once biometric data is captured, it frequently flows between governmental and private sector users. Companies have developed biometric systems to control access to places, products and services. Citizens can be asked for a thumbprint to access e-government services or enter a room in a corporate headquarters. Geolocation tracking, video surveillance and facial recognition software built on top of large biometrics collections can further enable pervasive surveillance systems.

After 9/11, many governments began collecting, storing and using biometrics identifiers in national IDs. Authorities justified these initiatives by arguing that biometric identification and authentication helps secure borders, verify employment and immigration, prosecute criminals, and combat identity fraud and terrorism. Despite this trend, the citizens of many countries have successfully opposed biometric national ID schemes including Australia, Canada, New Zealand, the United Kingdom, and the United

States.

Why You Should Oppose National ID Regimes

Mandatory national ID cards violate essential civil liberties. They increase the power of authorities to reduce your freedoms to those granted by the card. If a national ID is required for employment, you could be fired and your employer fined if you fail to present your papers. People without ID cards can be denied the right to purchase property, open a bank account or receive government benefits. National identity systems present difficult choices about who can request to see an ID card and for what purpose. Mandatory IDs significantly expand police powers. Police with the authority to demand ID is invariably granted the power to detain people who cannot produce one. Many countries lack legal safeguards to prevent abuse of this power.

Historically, national ID systems have been used to discriminate against people on the basis of race, ethnicity, religion and political views. The use of national IDs to enforce immigration laws invites discrimination that targets minorities. There is little evidence to support the argument that national IDs reduce crime. Instead, these systems create incentives for identity theft and widespread use of false identities by criminals. National ID cards allow different types of identifying information stored in different databases to be linked and analyzed, creating extreme risks to data security. Administration of ID programs are often outsourced to unaccountable companies. Private sector security threat models assume that at any one time, one per cent of company employees are willing to sell or trade confidential information for personal gain.

Biometrics Identifiers in a National ID Scheme are Irrational and Unnecessary

Arguments in support of biometrics rest on the flawed assumption that these ID schemes prevent identity fraud. Yet identity and authentication systems based on biometrics are weak because once these indicators are compromised, they cannot be reissued like signatures or passwords. You cannot change your fingerprints or your irises if an imposter is using this data. Up to five per cent of national ID cards are lost, stolen or damaged each year. Aggregated personal information invites security breaches, and large biometrics databases are a honeypot of sensitive data vulnerable to exploitation. Identity thieves can also exploit other identifying information linked to stolen biometric data. Those at the mercy of these databases are often unable to verify their security or determine who has access to them.

In some countries, stored biometric data can be obtained without a warrant and without notice. If you apply for a job that requires fingerprinting or a background check, your potential employer could require you to submit a photo to a biometric database used by police to identify people on the street. Photos and other information from data aggregators such as Facebook can be used to expand these databases. As facial recognition databases become larger and are used by more agencies to identify people, false positives — someone being misidentified as the perpetrator of a crime — will become an increasingly serious problem. Biometric databases also pose a mission-creep threat since the data can be used for secondary purposes.

Independent observers question whether expensive

biometric systems are as accurate as their proponents claim. There is not enough evidence to demonstrate the reliability and proportionality of this new technology.

Oppose Mandatory National IDs and Biometric Systems

Government mandated biometric systems are invasive, costly, and damage the right to privacy and free expression. They violate the potential for anonymity, which is crucial for whistleblowers, investigators, journalists, and political dissidents.

Along with NGOs, bloggers, and activists, EFF is fighting government proposals to integrate biometric information into centralized national ID schemes in several jurisdictions. We also condemn the use of biometric databases for law enforcement, e-government services, or private sector activities.

80 civil liberties organizations asked the Council of Europe in 2011 to investigate whether National ID biometrics laws in Europe comply with the Council of Europe Privacy Treaty and the European Convention on Human Rights. We refuse to let states collect massive amounts of biometric data without regard to privacy rights. EFF is currently working with allied organizations to oppose mandatory national ID cards and biometric databases in several countries.

RIGHTS.

DONATE TO EFF

ELECTRONIC FRONTIER FOUNDATION
eff.org