**Key points emerging policy issues in population registration**

Many UN Member States adopt different approaches to population registration and identity management. Issuance of a unique numeric identifier that ‘follows’ a citizen from ‘birth to grave,’ often accompanied by the issuance of a common identity document such as a national ID card, are considered normal practices in some parts of the world (*e.g. in much of Europe and the former Soviet space*), and are resisted in others (e.g. the furore over the abandoned national ID card scheme in the UK in 2010).

New forms of advanced digital registration systems are reducing the tendency of countries to manage separate, sometimes locally-administered databases with accompanying paper-based document issuance (*e.g. birth certificates, marriage certificates, tax and other ‘offline’ ID documents such as paper driving licenses, etc.*). In many western countries (e.g. Austria, Finland), as well as in some UNDP programme countries (*e.g. Afghanistan, Zambia, Sierra Leone*), more centralized systems of population registration have been or are being introduced involving both the issuance of a common identity card (*national ID card or registration card, many of which now have smartcard-enabled functions that can hold digital data not visible on the card*), and the merging of separate state population registration databases (*either by linking databases with a unique numeric identifier, or mandating the existence of a single centralized database, which the various state agencies can access according to their legally-determined needs*). It is not at all inconceivable that in the very near future, some UN member states may abandon cumbersome paper-based document issuance altogether, and instead simply add data fields to centralized national ID population registration system databases. These IT-enabled developments are unlikely to slow down, and are creating some fundamental political governance issues about the nature of the interaction between the state and its citizens on which no universal policy consensus exists. Some of these issues include:

1. Many states now run centralized population databases that contain not only identities verified by paper-based documents issued in pre-digital times, but identities verified by biometric data (*e.g. digital fingerprints, iris scans, facial images, etc.*). Submission of biometric data by the person to the state has not always been given voluntarily. Rather, it is often a condition of accessing other state services or accessing certain rights (*e.g. mandating digital fingerprint capture if a person wishes to register to vote*). It has also sometimes been given without people’s knowledge (*e.g. use of digital photograph/facial recognition software technology at immigration points/airports*).
2. Furthermore, use of centralized population registration and identity management places enormous responsibility on the state to ensure its accuracy and security. Although merging of state registration databases, with or without a national ID card, can obviously lead to synergies in how the state interacts with its citizens (*e.g. allowing for seamless decisions on healthcare access by cross-referencing social security data*), it also creates a ‘single point of failure’ should the data somehow be compromised (e.g. hacked from external sources, or manipulated internally). Centralized population registration and identity management, therefore, places enormous responsibility on the state to ensure:
   1. That an adequate legislative environment exists protecting use of personal data by state agencies. On the other hand, however, there is the duty of the state to protect itself and its citizens and thus there is passionate debate in many countries (evidenced by the recent Snowden case in the US) as to the extent to which person’s personal data can be mined and used for state security and anti-terrorism purposes.
   2. That personal data of persons is protected in the private and commercial spheres (e.g. protection against cyber crime, identity theft and the voluntary or involuntary transfer of data from state agencies to private sector bodies intent on data mining for commercial purposes).
   3. That an adequate legislative environment exists protecting the rights of citizens to know both what data, biometric and non-biometric, the state holds, and how that data is being used (freedom of information).
3. Increased use of biometric data and centralized population registration and identity management also significantly increases the amount of data that can be held. This opens up the possibility that, depending on the importance the political context places on non-biological elements of identity in a society such as religion or ethnicity, that such data fields can be captured and added to a person’s digital identity record (*there has been rigorous debate recently in Afghanistan on whether the separate ethnicities of ‘Pashtun,’ “Tajik,’ ‘Hazara,’ etc., should be added to the national ID card and its accompanying database)*. Similarly, other records such as whether a person has a criminal record or not can also be added to centralized databases. In conflict societies, therefore, or societies with difficult race or ethnic relations, etc., there is the possibility that governments could data mine population registration databases to cross-reference such data fields as ethnicity with criminal record. If manipulated for political reasons, this could create extremely tense scenarios.
4. Furthermore, some states are experimenting with the introduction of data readers that would allow police and other law enforcement personnel the possibility of ‘reading’ a person’s national ID document, which may contain data that the person himself is not even aware the document contains. Once again, in a conflict country, the potential of partial government officials having access to data that in previous eras was not available at short notice or without extensive and resource-consuming investigation is troublesome in the absence of adequate data protection environments.
5. Enhanced digital population registration and identity management certainly appears to increasing the importance of the *digital* identity of a person, as opposed to the ‘*natural*’ identity of the person confirmed earlier by paper-based systems. If, for example, there is somehow conflict between the data captured on a national ID card and the data on a birth certificate that cannot be resolved, states must make decisions as to which identity has primacy. Although such scenarios might seem to be insignificant, consider the possible effects of data being deliberately manipulated in order to amend, delete or add data to a person’s digital identity record that may not be accurate (*press articles showing the successful efforts of IT experts to hack the planned national ID card system in the UK in 2010, and add false data, generated intense debate that contributed to the abandonment of the system*).

1. Centralised population registration and identity management can, as earlier noted, however, create enormous synergies in the state’s efficient provision of services. IT advances can also make possible the documenting of citizens either not possible or comprehensives in previous times, often by allowing the *state to come to the citizens*, rather than requesting that *citizens come to the state* (e.g. registration for various services such as voter registration using agile, mobile technologies).
2. In the area of elections, UNDP has assisted approximately 9 African countries, as well as Bangladesh, with the implementation of digital voter registration system with biometric analysis capability in recent years. The UNDP Country Office in Yemen is currently assisting the Supreme Commission on Elections and Referenda in the forthcoming digital voter registration exercise in advance of both the referendum on the expected new constitution draft, as well as the next parliamentary elections. In Sierra Leone and Zambia, the UNDP Country Office is procuring major hardware and software infrastructure for the population registration systems, including national ID ‘smartcards.’ Lessons learned in these countries will prove invaluable in an area of governance work that is destined to grow substantially in coming years.