

Biometric technologies also enhance individual security by:

- Preventing imposters from claiming your identity and rendering personal identity theft obsolete
- Protecting personal data that is increasingly being stored online and in mobile devices
- Providing simple, easy means for government to ensure that the proper individuals are being served; and not being scammed by ill-intentioned, unauthorized imposters

Biometric technologies can also reduce waste, fraud and abuse by raising the bar on security and convenience for users by:

- Streamlining access to mobile applications
- Using biometrics to securely replace hard-to-remember passwords and IDs
- Obviating the need for so many individual IDs and easily cracked passwords
- Avoiding identity theft and the associated months-long recovery challenges
- Providing the opportunity for individualized services
- Speeding authorized people through checkpoints and border crossings
- Decreasing stigma of access to public aid programs
- Ensuring access by all citizens to qualified government benefits

Biometric technologies “enables,” rather than “limits,” access and quality of services for both users and providers by:

- Ensuring only qualified people are provided benefits
- Lowering the costs of immigration control at border crossings by means of automated e-gates and biometric identification
- Using biometrics to narrow the scope of kinship investigations for immigration and adoption purposes
- Developing ways of quickly uniting relatives with loved ones in disaster situations
- Producing credentials for first responders to enable quick access to disaster areas
- Improving remote access to benefits and services, reducing travel costs and associated energy consumption and pollution

And biometrics can do all this and yet preserve user privacy as:

- No one else can gain access to your personal data because no one else has your unique biometric attribute that permits access
- The risk that a person can steal your identity and, posing as you, collect benefits; board an airplane; get a job; gain access to your personal data, etc., is greatly reduced or eliminated
- Systems or services provided by Government or business could easily be created in such a way as to allow users to opt in or opt out if they felt that privacy was in any way being challenged. A user’s right to privacy need not be infringed. Systems could easily be set up in such a way as to allow those of us who wish to take full advantage of government services to opt in. Those who choose to opt in are not surrendering their right to privacy. They are simply acknowledging that it is reasonable for them to surrender their right to anonymity. We are, and should always be,

guaranteed our right to privacy but there is no right to anonymity if goods or services are being provided for us or to us. These services are by definition based on user identity.

In short, the role of biometrics in protecting user identity, guaranteeing that goods and services are making their way only to bona fide recipients, and reducing fraud and abuse is without equal. For only by knowing “who” with some high degree of certainty can government or business ensure that only those entitled are being served. To do otherwise is both an economic and social injustice, as biometrics technology has now advanced to a level where the performance is proven and the benefits are real and measurable, and easily outweigh the costs.