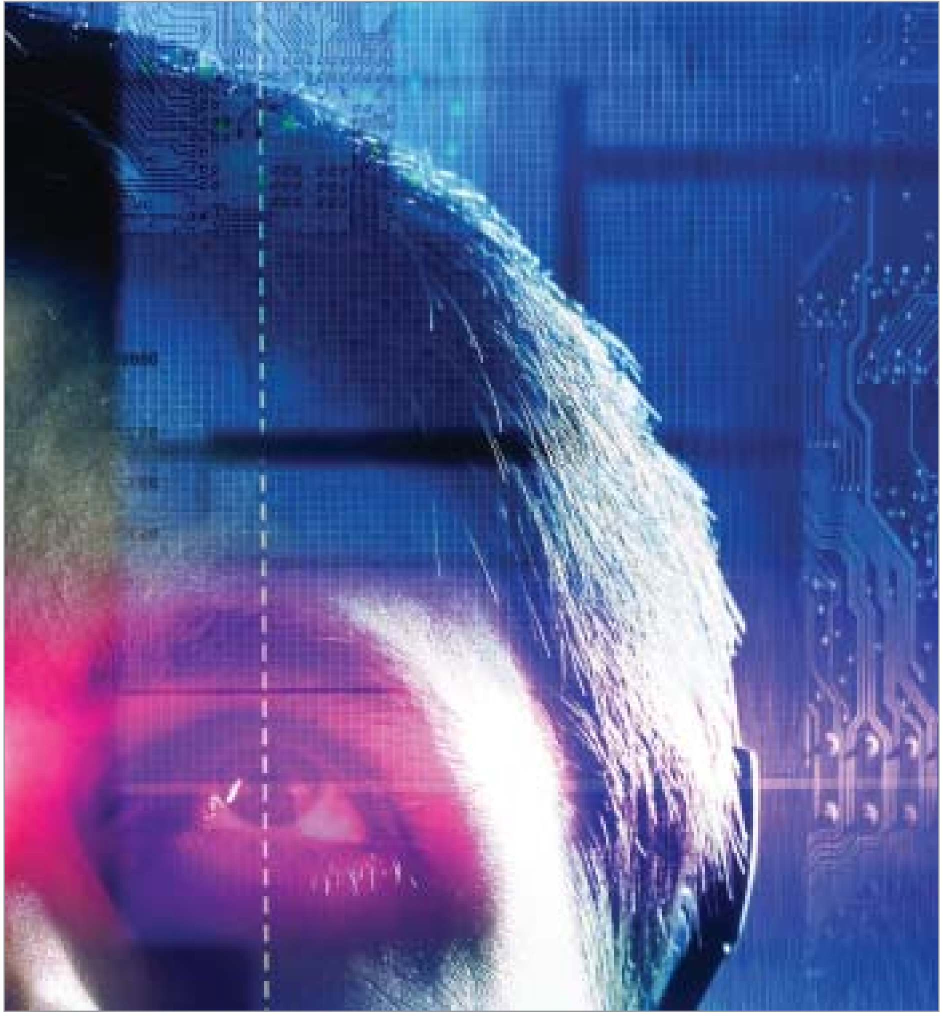
Collision Course:
Biometrics and Rights Management

By C. Maxine Most

Biometrics can tie rights management to individuals, solving many problems of portability. The widespread use of biometric authentication, however, poses significant technical, social and legal challenges. Among these are issues of ownership and use rights of the biometric data itself. These must understood if widespread adoption is to occur.



The worlds of Digital Rights Management (DRM) and biometric technology appear to be on a clear but circuitous collision course. There are two concurrent paths upon which this inevitable collision will occur. The first, and in many regards the more obvious, is where man meets machine in ever more sophisticated rights management strategies. To truly connect access, management, distribution and use of digital content to authorized individuals, there must be a way to bridge the human-digital divide. Biometrics is really the only way to be certain that a claimed digital identity is indeed associated with a particular human being. The second, and in many ways more intriguing path, is considering the digital rights associated with the actual biometric information itself – those of ownership, access, distribution and ultimate control of an individual's own biometric data.

Machine-to-Machine versus Human-to-Machine interfaces

Biometrics (human-based physiological and behavioral identification technologies) have generally been ignored by the rights management community. The term may come up in a theoretical paper or during a conference panel discussion on the future of rights management, but to date, biometrics are considered a novelty, if they are considered at all. Even then, they are peripherally relegated to "add-on" status – something that can be attached after the true work of developing and deploying a rights management system is complete, or that is assumed to be part of some future authentication infrastructure.

To be fair, the emerging rights management market is struggling for mainstream status and has therefore focused on identifying substantial market opportunities and working through infrastructure and machine-to-machine authorization and authentication issues. However, the human-to-machine authorization and authentication issues are looming and they are potentially far more complex. Biometrics will come into play after the machine-to-machine rights management models play out and the human-to-machine interface becomes the final driving process issue.

The real concern … is the potential harm to an individual if their biometrics are unknowingly captured and templates are created.

Latent Integration

Integrating biometrics into existing systems – both from a human interface and infrastructure design perspective – is a complex and rigorous process. This ultimate link between the digital and human management of identities, therefore ought to be a critical aspect of any well-architected digital rights system. Biometrics are more than just a method of authentication, but rather central to the way a system functions and the way humans will interact with it. Proven evolving methods of machine-to-machine authorization and authentication will continue to be the foundation of many DRM implementations. However, it is the human-to-machine authorization and authentication that can be messier, less controllable, and subject to misunderstanding, non-compliance, confusion, environmental constraint and old fashion human error. In this regard, biometrics are not simply peripheral add-ons. These threshold-based human-to-machine interfaces technologies require a high level of sophistication in their successful application and tend to expose weaknesses in security processes and programs that fail to properly assess and profile risk. This human-machine authentication link must therefore be more fully integrated – from the beginning - for long term success of rights management systems.

Data Ownership

Biometrics employed within the context of a rights management scheme (or for any other authentication purpose) will likely exacerbate digital rights issues. In general, rights management is associated with copyright enforcement and protection of Intellectual Property (IP) associated with commercial, corporate and academic content. However, the ownership rights in regards to biometrics have more far reaching implications.

The question who owns my biometric data? - who owns the image (digital representation of a finger, iris, face or the dynamic variables associated with a voice or signature) or who owns the template (mathematical representation of this image) – may at first appear deceptively simple. It may seem trivial to confidently assert that every individual owns their own biometrics. That this is data of a most intense personal nature and an individual ought to control it. Unfortunately, this is not the case.

Every day individuals leave a trail of biometrics - fingerprints on everything from coffee mugs to computer keyboards, voices on telephone message systems, faces on dozens of camera and video capture devices. To a certain extent, our biometric image data is being made freely available and collected on an ongoing basis.

A recent radio news story reported about a young woman who was horrified to discover her face on someone else's body at an adult website. She had no idea how or where she had been photographed. The proliferation of digital cameras – particularly in mobile phones - has made capturing this sort of personal digital information (as well as commercial images of a proprietary nature) effortless. So, with the expanding use of biometric information in government and commercial applications (passports, border control, bank access, Point-Of-Sale, etc.), the question of digital rights is quickly extending beyond commercial, corporate, or academic copyright and IP boundaries into the realm of personal ownership of the biometric markers that uniquely define each and every human being.

Data Protection

Furthermore, this biometric image data can be used– with or without permission - to create accurate biometric templates. Does the individual who captured the image or whose body it belongs to own this image data and the associated templates that can be generated from it? In the US, the capture of such images, including photos and voice data, in public places has repeatedly been held to be constitutional by the US judicial system. It is not considered a privacy violation unless it is done without consent within the confines of an individual's home. So there is a case to be made that biometric image data is not exclusively owned by an individual.

However, it would seem that creating a biometric template from this data is another matter. It seems reasonable to assume that creating biometric templates with the intent to perform an illicit or fraudulent activity would be illegal under recent US legislation designed to address identity theft. But is the act itself either

The ownership rights in regards to biometrics have more far reaching implications.

illegal or a direct privacy violation? The US legal system has a long way to go to catch up with biometric technology, though some states have or are considering passing legislation protecting biometric data. The state of New Jersey recently passed such a law, but it is yet untested.

Unlike the prolific case history for IP copyright protection, biometric data ownership is brand new territory, at least in the US. Europe, however, has a much stronger legal foundation for the status of biometric data. European data protection laws ensure that individuals own their personal data, must be informed of and consent to it's collection and that this data may only be used for the express purpose for which it was collected. Though this law has not been tested in specific regards to biometrics, the implications are clear.

Bottom Line

The real concern beyond any legal definition is the potential harm to an individual if their biometrics are unknowingly captured and templates are created. What can someone with ill intent do while in possession of another person's biometrics data? In reality, without a direct link to an individual's personal information, biometric images and templates in and of themselves are pretty much useless. The images are only good to generate templates and, at least for now, there a wide range of technologies and algorithms to create templates.

Biometric template data is statistical in nature – not exact – so using an identical copy of an existing stored template would automatically be considered a fraud attempt. It is really the potential linking of images with the biometric capture device and template generating algorithms along with individual personal data that holds the potential for privacy invasion and security risk. This risk is mitigated by distributing the storage of these types of data, and can be further mitigated by applying a distributed network architecture to identity based applications that maintain this separation as the data is accessed and processed by the system. (See the October 2002 edition of Biometrics Marketing Intelligence for more on distributing ID networks.)

How authentication works essentially defines the way the network works.

The emergence of identity as a fundamental component of next generation global computing infrastructure escalates authentication concerns from afterthought status to primary driver. How authentication works essentially defines the way the network works. Constructing a rights management infrastructure that can truly support identity poses significant technical, social and legal challenges. It does, however, offer a vision of biometrically enabled identity based DRM (and more broadly identity management) networks that provide the foundation for addressing the use and misuse of personal, civil, corporate and commercial digital rights assets–including our biometric identities.

The use of biometrics is therefore an integral part of the ever more complex digital rights management matrix. What might at first seem to be a peripheral aspect of architecting a system and providing the human-to-machine link, in and of itself adds a whole other dimension to managing information. ■

C. Maxine Most is the Principal of Acuity Market Intelligence (www acuity-mi.com), an emerging technology market research and analysis firm and the Editor of Biometrics Market Intelligence (BMI) (www.biometricsmi.com), a quarterly report providing market insight and analysis for the biometrics industry. For more information Ms. Most may be reached at cmaxmost@acuity-mi.com.