Abstract Today's "new technological realities" force us to examine, from the law and policy perspectives, what is required to safeguard the public interest and to ensure optimal results for society. Biometrics is one such new technology reality. While not enjoying the media stature and public controversy associated with high tech issues like genetic cloning and cyberspace, biometrics -- which seeks a fast, foolproof answer to the questions, "Who are you?" or "Are you the person whom you claim to be?" -- will cause the law to take notice as it becomes more extensively used in the public and private sectors. Businesses, numerous government agencies, law enforcement and other private and public concerns are making increasing use of biometric scanning systems. As computer technology continues to advance and economies of scale reduce costs, biometrics will become an even more effective and efficient means for identification and verification. After briefly discussing biometric technologies and biometric applications, this chapter defines privacy in the context of biometrics and discusses which specific privacy concerns biometrics implicates. This chapter concludes that biometrics is privacy's friend because it can be used to help protect information integrity. The author also contends that any legitimate privacy concerns posed by biometrics, such as the possibility of a secondary market in individual biometric identification information, can be best handled by the existing law and policy framework. The author next considers the future of biometrics, and contends that "biometric balkanization," or the use of multiple biometric technologies deployed for multiple applications, provides greater privacy protections than does biometric centralization, or the use of one dominant biometric technology for multiple applications.

Keywords: Privacy, biometric law, public policy, government, information policy, constitutional law.
1. Introduction

On May 18, 1997, in his commencement address at Morgan State University, President William J. Clinton stated:

The right to privacy is one of our most cherished freedoms. As society has grown more complex and people have become more interconnected in every way, we have had to work even harder to respect privacy, the dignity, the autonomy of each individual . . . [w]e must develop new protections for privacy in the face of new technological reality [1].

While it is doubtful that President Clinton had biometrics in mind during that Sunday speech, biometrics is clearly emerging as one such "new technological reality." From activities as diverse as the Winter Olympics in Nagano, Japan to the prisons of Cook County, Illinois, both the public and private sectors are making extensive use of biometrics. This new technological reality relies on "the body as password" for human recognition purposes to provide better security, increased efficiency and improved service [2,3,53,54]. As the technology becomes more economically viable, technically perfected and widely deployed, biometrics could become the passwords and PINs of the twenty-first century. In the process, biometrics could refocus the way Americans look at the brave new world of personal information [4].

Understanding biometrics is thus essential for elected officials and policymakers charged with determining how this new technology will be used and what role, if any, government should play in its regulation. Familiarity with biometrics is also important for the legal, business and policy advocacy communities so that they can meaningfully participate in the public debate related to biometrics.

Similarly, understanding the law and policy concerns of biometrics is necessary for the engineers and scientists who have brought about this new technological reality. History teaches us that new technologies, created by engineers and scientists, spark new law and cause old legal doctrines to be rethought, rekindled and reapplied by the nation's law and policy makers.2

New technology can cause a creative reshaping of existing legal doctrine when, for example, the judiciary has embraced a technology more quickly than the legislature, the executive branch or even the actual marketplace for the technology. To consider a well-known example from the legal casebooks, in 1928, there was no law or regulation requiring coastwise seagoing carriers to equip their tugboats with radio receiver sets. Moreover, no such custom or practice existed in the maritime industry, despite the fact that such sets could easily be used by tugs at sea to receive storm weather warnings. In a landmark legal case, Federal Circuit Judge Learned Hand, one of the great American jurists of this century, deemed that tugboats without radio receiver sets were unseaworthy because "a whole calling may have unduly lagged in the adoption of new and available devices" [6]. By accepting a new technology -- in this case, wireless communications -- more quickly than the legislative and executive branches or even the affected industry, Judge Hand, in effect, creatively reshaped the law. No longer would strict adherence to local custom and industry practice offer a

---

1 This chapter is largely based on a previously-published article by the same author: John D. Woodward, "Biometrics: Privacy’s Foe or Privacy’s Friend?" in Proceedings of the IEEE, Sept. 1997.

2 For an excellent examination of the intersection of science and technology with law and policy, see [5].