**You have been approached by a legislative staffer who is interested in drafting a bill on face recognition technologies. What issues would you highlight for the staffer?**

Three challenges apply to *any* face recognition system. First, does the software have high accuracy? If not, any process that relies on the software will be, at best, ineffective and, at worst, harmful. Second, are mistakes concentrated among certain protected classes? For example, face recognition software trained on mugshots and used in the criminal justice system risk matching African American men at overly high rates. Finally, is the data fueling the system being handled responsibly? To respect a user’s privacy and autonomy, they must consent to their face being used, be told what it will be used for, and be able to remove their face in the future. Security is also crucial because once biometric data is lost, it cannot be deidentified.

One must also consider the context within which the software is being used. Face recognition technologies used by the government for security purposes is of particular concern. If executed irresponsibly, this practice could severely limit first amendment (freedom of speech) and fourth amendment (unreasonable search and seizure) rights. Face recognition allows the government to surveil public spaces, which scares Americans away from protests and other public debates. Moreover, the opportunistic nature of assembling large datasets means that individuals often do not consent to the government using these images in criminal investigations. Ensuring a face recognition system uses responsibly handled data to make accurate and unbiased predictions is a necessary, but insufficient, component of ethical software – the social and legal system must be considered on a case-by-case basis.