International Communication Association Annual Conference, 2013 (London)
Law & Policy Division

Jenifer Sunrise Winter

Cloud-based facial recognition: Establishing the citizen at the center of policy and design

Introduction and background

This paper argues that data collection via cloud-based facial recognition technologies poses a grave threat to privacy, potentially hindering free speech and democratic discourse, and that related policies and systems must focus on citizens' perceptions of appropriate use of personal data.

Expanding global media enterprises and an array of technical changes, including the proliferation of mobile devices and public surveillance cameras, "Big Data" aggregation and mining of personal information, a move to cloud-based storage and processing, user-generated data and tagging, the emergence of semantic web standards, and the sophistication of facial recognition systems have led to cloud-based facial recognition (Keller, 2011) that enables mobile devices to near-instantaneously match subject images to online identity profiles. Acquisti, Gross, and Stutzman (2011) describe experiments where they were able to match unidentified, pseudonymous profile photos of subjects from an online dating site with their Facebook photos, as well as matching students walking around college campuses with their online records using an Internet-enabled mobile device. Related technologies are already employed by large media corporations such as Facebook, and marketers are employing them in billboards, vending machines, televisions, and home gaming systems in order to gauge viewer affect and offer customized products (Wadhwa, 2012). This behavioral data will likely be linked to other personal information via unique identification systems in the future. Law enforcement agencies are also employing advanced facial recognition systems, and they are a core component of the United States' Next Generation Identification program. It is expected that the sophistication and reach of these technologies will continue to grow as we move towards next-generation standards for the Web and increased data aggregation and mining.

Counter-argument

Proponents of facial recognition technologies argue that they will lead to increased security and customer convenience. The United States Federal Trade Commission (FTC) recently released a best practices report advocating the use of Fair Information Practice Principles (FIPPs) and relying on industry self-regulation. FTC Commissioner J. Thomas Rosch dissented, arguing that any envisioned harms were not substantial or tangible, and that there is, as of yet, no means to establish that harms may occur. Thus, companies should not be required to provide an opt-out choice when these technologies are used. He claimed that the FTC will be able to keep up with the rapid pace of technological change related to facial recognition (Federal Trade Commission, 2012).

Argument: Cloud-based facial recognition

My argument against the self-regulated use of cloud-based facial recognition technologies is based on several factors. First, cloud-based facial recognition provides a system of unique identification that allows the aggregation and mining of personal information. It does so more effectively than any other biometric method, and requires only a camera-equipped mobile phone and Internet connection. Second, even if system designers and data managers choose to follow the FIPPs, there may be no way to truly opt-out of these systems or to constrain their use. One does not necessarily know that cloud-based facial recognition is being employed, and may not be able to give consent. Whether one actively uses the Internet or not, facial recognition systems enable one to be linked to numerous public records and online profiles. Further, these will likely include health-related data and will link everyday activities to the previously-protected realm of medical information. In the United States, context-specific laws such as HIPAA protect medical information, but facial recognition-enabled data aggregation will link this to the larger, and less restrictive, domain of search and purchasing behaviors linked to the Web. In doing so, it may also expose political behaviors, or any personal information that could be used by corporations or governments to disadvantage certain individuals or groups. This has a great potential to lead to political and economic discrimination, or limit freedom of access to information or discussion of issues relevant to democratic decision-making (Winter, 2012). Civil liberties and constitutional freedoms will be threatened, as this will contribute to a society where citizens cannot freely express their opinions without being publically identified and monitored. These developments threaten to destroy any sense of anonymity when engaging in public affairs, and therefore pose a grave risk to public participation in democratic discourse.

What needs to change?

While facial recognition technologies are currently under study by the Federal Trade Commission due to consumer privacy concern (Federal Trade Commission, 2011, 2012), these technologies are rapidly entering the marketplace with little oversight. Contrary to Commissioner Rosch's dissenting argument, industry self-regulation in the United States has not been successful in protecting personal information. Lacking any meaningful and enforceable legal recourse, corporations and governments are unlikely to handle citizens' data in a conscientious manner. Further, too many questions remain about the accuracy and reliability of data aggregation, and the ability to secure data once it is gathered. As both corporations and governments move to collect and store more personal information, the tension between personal privacy and open data initiatives will continue to grow. The time to create legal protections is before major problems arise (Weber & Weber, 2010). Measures to protect citizens' ability to opt-out of facial recognition systems and to protect personal data should be implemented and enforced *before* they are widespread.

Existing conceptions of privacy are not capable of addressing the radical changes brought about by cloud-based facial recognition. Increased research that takes into account the specific context of use (e.g., Nissenbaum, 2010) is necessary to understand citizen concern and to develop systems and policies that accord with social norms and expectations. As designers of systems and policies work to design technical standards, regulations, and laws, more attention should be placed on the experience of citizens in managing personal data flows. We require a more nuanced understanding of how cloud-based facial recognition systems will affect existing political and social relationships and must determine in what instances the collection and analysis of these data is relevant or necessary.

References

Acquisti, A., Gross, R., Stutzman, F. (2011). Faces of Facebook: Privacy in the age of augmented reality. Black Hat 2011. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf.

Federal Trade Commission. (2011 November 21). FTC announces agenda, panelists for facial recognition workshop. http://www.ftc.gov/opa/ 2011/11/facefacts.shtm.

Federal Trade Commission. (2012 October 22). Dissenting Statement of Commissioner J. Thomas Rosch, Issuance of Federal Trade Commission Report, Facing facts: Best practices for common uses of facial recognition technologies. Washington, DC: Federal Trade Commission.

Keller, J. (2011 September 29). Cloud-powered facial recognition is terrifying. *The Atlantic Monthly*. http://www.theatlantic.com/ technology/archive/2011/09/cloud-powered-facial-recognition-is-terrifying/245867/.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, Ca.: Stanford University Press.

Wadhwa, T. (2012 Aug 8). What do Jell-O, Kraft, and Adidas have in common? They all want to know your face. Retrieved from http://www.forbes.com/sites/singularity/2012/08/08/ billboards-and-tvs-detect-your-face-and-juice-up-ads-tailored-just-for-you/

Weber, R.H., & Weber, R. (2010). *Internet of Things: Legal perspectives*. Berlin: Springer-Verlag Berlin Heidelberg.

Winter, J. S. (2012). Privacy and the emerging Internet of Things: Using the framework of contextual integrity to inform policy. Refereed paper published in the Pacific Telecommunications Council Conference Proceedings 2012. Honolulu: Pacific Telecommunications Council.