2013

Face-to-Data -- Another Developing Privacy Threat?

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Brussels Privacy Hub

Christopher Millard
Cloud Legal Project

Dan Jerker B. Svantesson
Bond University

Editorial

Face-to-data—another developing privacy threat?

Christopher Kuner*, Fred H. Cate**, Christopher Millard**, and Dan Jerker B. Svantesson***

The constant development of technology gives rise to an equally constant stream of privacy issues. One of the most interesting recent developments is what we can call face-to-data (F2D). F2D refers to at least partially automated processes for accessing personal information about a person based on an image of that person's face.

Ground-breaking research by a team of researchers from Carnegie Mellon University has highlighted that advances in face recognition technology, combined with the widespread posting of images linked to names on, for example, social media sites, and the processing power provided by advances in cloud computing, create a new set of privacy issues,[1] similar to, but also distinct from, traditional privacy issues associated with facial recognition.

The Carnegie Mellon University team ran a series of experiments. For example, using a search tool, they built up a database of images and names collected from publicly available Facebook profiles. They then captured images of consenting students and ran those images through off-the-shelf face-recognition software, linking in the data gained from the Facebook profiles. In the test, about a third of the students were identified.

The Carnegie Mellon work is striking because it uses commonly available devices (ie an iPhone) to perform highly effective facial recognition using candid photographs, and then links those to a series of databases to generate an immediate response. So, for example, a person may use a phone on a street, take a picture, and within seconds have back the Social Security Number and street addresses of the people photographed. Information that can then be used to, manually or through automated processes, extract further personal data about those people.

In light of this, the facial recognition aspect is only one part of the overall process of concern here, and facial recognition as such is a broader phenomenon than F2D. Thus, to properly understand the phenomenon we are dealing with, it is undesirable to discuss F2D merely as a facial recognition issue.

F2D can of course serve a variety of goals ranging from government surveillance, to business use and to satisfy personal curiosity, and it is interesting to consider how current data privacy laws address F2D. And with privacy laws being developed or changed in so many parts of the world, it is even more interesting to consider how the next generation of data privacy laws will address F2D.

As is well known, the privacy regulation of today is largely focused on data use that falls outside the private sphere; that is, in those countries that do have some form of privacy regulation in place, there is typically some form of exemption for data use in the context of the 'private affairs' of individuals. This means that in most countries, while F2D for business purposes *may* be regulated, personal use would typically be unregulated. Furthermore, even in those countries, such as within the European Union, where commercial use may fall under applicable data protection schemes, it may be possible to circumvent the regulatory impact by placing a simple notice onsite informing potential customers of the use of F2D at that location, and then assuming that their failure to object to the processing should legitimize it.

The conclusion is that traditional data protection regulation provides limited comfort for those concerned about the impact of F2D. While there have been some improvements to the rules governing consent in the EU General Data Protection Regulation proposed by the European Commission in January 2012, it seems unlikely that even the world's most modern and protective legislative initiative will satisfy fully those fearing the privacy impact of F2D.

* Editor-in-Chief
** Editor
*** Managing Editor

1 The highly interesting research findings have been presented by Alessandro Acquisti at various conferences, including IAPP Europe Data Protection Intensive 2012 (April 2012) and the IAPP Privacy Academy 2012 (October 2012). For more information about the research, see: <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/>, accessed 30 October 2012.

Many people may view F2D as a 'cool' new technology tool. But critics may question the societal benefits this technology has to offer. In the end, a widespread private use of F2D may contribute little to society while presenting a significant risk of potential harm to privacy. In light of this, some may go as far as to argue that, with F2D we have finally reached a stage where the technology in question is so 'creepy' that it does not matter whether it is merely being used for 'harmless' curiosity.

F2D can also be seen to have highlighted a gap in the coverage of privacy regulations that focus more or less exclusively on the conduct of business operators, governments, and organizations. F2D may suggest a need for a new level of data regulation of personal use of other persons' personal data. If such a regulatory response cannot be developed, and if inadequate steps are taken to restrict the use of F2D, then privacy advocates may call for the recognition of a fundamental right of anonymity.

In the end, F2D may best be viewed as just another example of how technology is developed based on what technology *can* do. Should the focus instead be shifted more to what the technologies we develop *should* do? [2]

doi:10.1093/idpl/ips032
Advance Access Publication 6 December 2012

2 For a deeper discussion of this topic see: D Svantesson, 'Face-to-data—the ultimate privacy violation?' (July 2012) 118 Privacy Laws & Business 21–4.