TESTIMONY

Professor Alessandro Acquisti
Heinz College and CyLab, Carnegie Mellon University

Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
U.S. Senate

What Facial Recognition Technology Means for Privacy and Civil Liberties

Wednesday July 18, 2012

Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee: I am honored to appear before you today. I am a tenured associate professor at the Heinz College, Carnegie Mellon University (CMU), a member of CMU CyLab, and the co-director of CMU's Center for Behavioral Decision Research (CBDR).[1] I am an economist by training (I hold Master degrees in economics from Trinity College Dublin and from the London School of Economics), and I am interested in how economics can help us understand the impact of information technology (I hold a PhD in Information Management and Systems from the University of California at Berkeley). For about 10 years, I have been studying the economics and behavioral economics of privacy. My research in this area has combined economics, experimental behavioral decision research, and information technology to investigate the trade-offs associated with the protection and disclosure of personal information, the technologies that enhance the former or the latter,[2] and how individuals value, and make decisions about, those trade-offs.[3]

My remarks in this testimony will concern research that I and others have carried out in the field of privacy and face recognition.[4] I became interested in face recognition indirectly, as a result of my studies of privacy and online social networks, which started in 2005.[5] In the summer of 2011, together with my colleagues Dr. Ralph Gross (a face recognition expert at Carnegie Mellon University) and Dr. Fred Stutzman (an online social networks expert also at Carnegie Mellon University), I presented the results of a series of experiments about the privacy implications of the convergence of more accurate face recognition technology, increasing public availability of personal data (including digital photos), and statistical re-identification techniques.[6]

In my testimony, I will highlight four conclusions from my and other scholars' research in this area:

First, face recognition is "now." The technology has evolved over several decades. While early algorithms vastly underperformed human ability to detect and recognize faces, modern ones have progressed to a point that they are now being deployed in end-user applications.

Second, the convergence of face recognition, online social networks, and data mining has made it possible to use publicly available data and inexpensive off-the-shelf technologies to produce sensitive inferences merely starting from an anonymous face. I will highlight the results of three experiments we conducted in this area, including one in which we predicted portions of the Social Security numbers of students at a North-American college starting from photos of their faces.

Third, face recognition, like other information technologies, can be source of both benefits and costs to society and its individual members. However, the combination of face recognition, social networks data, and data mining, can significantly undermine our current notions and expectations of privacy and anonymity.

Fourth, depending on which goals Congress intends to achieve in the area of face recognition, different policies and interventions may be considered. If the privacy and civil liberties implications of face recognition are the concern, it is unlikely that industry solutions alone (such as self-regulatory efforts) will address those concerns.

1. The State of Face Recognition Research

Research in computer face recognition has been conducted for over forty years.[7] For most of this time, computers underperformed humans in tasks involving the detection and recognition of individuals through their faces. But the progress of algorithms has been steady: since 1993, the error rate of face recognition systems has decreased by a factor of 272.[8] Today, under certain conditions, machine face recognition performance can be comparable or even better than humans at recognizing faces.[9]

As face recognizers' accuracy kept increasing, face recognition started being deployed in more products and services. About 10 years ago, face recognizers remained the domain of government agencies or large corporations, and were mostly used in security and police activities.[10] In the past few years, face detection, face recognition, and other related algorithms (such as the estimation of individual traits from facial images) have started appearing in end-user products, and in particular Web 2.0 services. Following the acquisition of Neven Vision in 2006 and of Like.com in 2010, Google has offered Picasa users face recognition tools to organize photos according to the individuals in them.[11] Apple's iPhoto has employed face recognition to identify faces in a person's album since 2009.[12] Using Face.com's licensed technology, Facebook has used face recognition to suggest "tags" of individuals found in members' photos.[13] Klik, also developed by Face.com, used face recognition to allow real time tagging of Facebook friends through the same mobile camera used to take their pictures.[14] NEC has designed billboards that automatically locate faces of people passing by and estimate their gender and age, in order to target advertising accordingly.[15] SceneTap uses face detection to estimate the size of and gender ratio in a crowd of patrons at a venue – and allows individuals who downloaded its app to find that information online.[16]

Under typical, real life conditions (for instance, when facial shots are not captured in well-lit conditions or through frontal, "mugshot" poses) computer face recognition still underperforms humans. As we further discuss in the next section, however, face recognition's limitations are more transient than systemic: given the growing commercial interest in face recognition and its application, the gap between humans and machines in recognizing faces is likely to keep diminishing.

2. How to Predict Someone's SSN Starting From Their Face

As a privacy researcher, a few years ago I became interested in the privacy implications of the convergence of two trends: the improving ability of computer programs to recognize faces in digital images, and the increasing public availability of identified facial photos online - especially through online social networks. In a study with Ralph Gross and Fred Stutzman presented in the summer of 2011,[17] we investigated whether the combination of publicly available Web 2.0 data and off-the-shelf face recognition software may allow large-scale, automated, end-user individual re-identification. We identified individuals online across different services (Experiment 1); offline – that is, in the physical world (Experiment 2); and then inferred additional, sensitive information about them (their interests and their Social Security numbers), combining face recognition and data mining, thus blending together online and offline data (Experiment 3); finally, we developed a mobile phone application to demonstrate the ability to recognize and then predict someone's sensitive personal data directly from their face, in real time, on a mobile device.

In the first experiment (Experiment 1) we investigated online-to-online re-identification. We took unidentified profile photos from a popular dating site (where people use pseudonyms to protect privacy), compared them - using face recognition - to identified photos from a popular online social network (Facebook; namely, we used the component of a Facebook profile that can be publicly accessed via a search engine; in other words, we did not even need to log on to the network itself). Through this process, we were able to re-identify about 10% of the pseudonymous members of the dating site.

In the second experiment (Experiment 2) we investigated offline-to-online re-identification. Its methodology was conceptually similar to that of Experiment 1, but in this case we attempted to re-identify students on the campus of a North American college. We took photos of them with a webcam and then compared those shots to images from Facebook profiles. Using this approach, we re-identified about one third of the subjects in the experiment.

The first two experiments illustrate how third parties can use publicly available data not just for contextual identification (linking images of the same person in an album of photos) but also for universal, unique identification.[18] In the final experiment (Experiment 3), we predicted the interests and the first five digits of Social Security numbers (SSNs) of some of the individuals who had participated in the second experiment. We did so by combining face recognition with the algorithms we developed in 2009 to predict SSNs from public data.[19]

In the context of Experiment 3, SSNs were merely one example of the many types of information it is possible to infer about a person, starting merely from an anonymous face, through a chain of inferences in a process of *data accretion*.[20] The process illustrates the privacy implications of face recognition technology, and can be summarized in the following manner: First, face recognition links an unidentified subject (for instance, a face among many in the street) to a record in an identified database (such as an identified photo of the subject on Facebook, LinkedIn, Amazon, or in a state's DMV database). Once the link has been established, any online information associated with that record in the identified database (such as names and interests found in the subject's Facebook profile; or demographic data found on Spokeo.com - a social network and data aggregator) can in turn be probabilistically linked to the unidentified subject. Lastly, through data mining and statistical re-identification techniques, such online information can be used for additional, and much more sensitive inferences (such as sexual orientation,[21] or Social Security numbers[22]), which, in turn, can be linked back to the originally unidentified face. Sensitive data is therefore linked to an anonymous face through what we may refer to as a "transitive property" of (personal) information - a process that merely requires publicly available data. Sensitive information thus becomes "personally predictable information."

As a further example of what is already possible to accomplish using existing technologies and publicly available data, we developed a mobile phone application which, once a photo is taken of a person's face, uploads it to a server; there, a program compares it to a database of images downloaded from the Internet – and tries to recognize the person; thereafter, using the same process adopted in Experiment 3, the program attempts to predict the person's sensitive personal information, and finally displays that very same information on the device's screen, overlaid on the face of the subject. Essentially, this application (which we demoed at a security conference in August 2011, with no intention of making it publicly available) demonstrates that it is possible to conduct on a mobile device and in real time the process of Experiment 3.

We use the term *augmented reality* to describe that application: it refers to the merging of online and offline data that new technologies make possible. If an individual's face on the street can be identified

using a face recognizer and identified images from social network sites such as Facebook or LinkedIn, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her.

2.1 Current Limitations and Why They Are Transient

Our experiments, while successful, were constrained geographically (we focused on the population of a North-American city, and the students at a North-American college campus) and in scope (we used databases with up to a few hundred thousands of images). The results we obtained are not *yet* scalable to the entire American population for a number of reasons: First, computational costs: we estimate that comparing the shot of a person's face to a database with mugshots of 280 million US residents aged 14 years or older, using the same hardware as in our experiments, would take over four hours (rather than the few seconds that process took in our experiments). Second, "false positives:" when comparing millions of human faces, several individuals' faces will be similar to each other, and computers do not yet excel in separating a face of a person from a face of someone who looks very much like that person. Third, light conditions, facial hair, or non-frontal poses impair the accuracy of machine face recognizers. Fourth, photographic images (and in particular frontal mugshots) may not be available for the entire population.

Those hurdles, however, are being progressively overcome. They are transient, not systemic. First, as computers' processing power keeps increasing, and cloud computing costs decrease, it will become more efficient to run end-user applications on mobile devices similar to the one we developed, for mass-scale, automated, peer-to-peer face recognition. Second, false positives will likely keep reducing, as machine face recognition error rates are decreasing by one half about every two years.[23] Third, researchers are actively working on improving computers' ability to recognize faces under varied conditions of light, facial hair, and poses. Fourth, entities such as online social networks are amassing some of the largest known databases of identified photos, from which increasingly accurate biometric models or "faceprints" of increasing portions of the US population can be, and are being, built.

It is likely, therefore, that within a few years, real-time, automated, mass-scale facial recognition will be technologically feasible and economically efficient. It will be feasible for individual end-users, in a peer-to-peer fashion; it will be feasible for firms (both for companies, such as online social networks, that will actually own the data; and for third parties that will rent identity recognition services from or through the former); and it will be feasible for governments that will access or trade biometric data with

the private sector. In this world, “facial searches” in the street may become as common as text-based queries on search engines are today.

However, the fact that real time recognition technology may be used, in principle, by individuals, firms, and governments alike, does not guarantee that, in practice, all parties will gain equal access to it. The parties in actual possession of the largest databases of images will be in the better position to make use of face recognition technology and control the access that others will have to it. Similarly, the parties with more resources will be those more likely to be able to exploit it, or avoid being exploited by it.

3. Trade-offs and Privacy Concerns

In economic terms, privacy shares the characteristics of both an *intermediate good* (a good that is valued in an instrumental way, because of its consequences: for instance, loss of personal data can cause identity theft and ensuing economic damage), and a *final good* (a good that is valued for its own sake: for instance, ubiquitous surveillance creates discomfort).[24]

I will first discuss the implications of face recognition for privacy as an intermediate good. As it is often the case with advances in information technology, the ramifications of cheap, powerful facial recognition technology in the hands of individuals, firms, and government agencies, are complex. They include both scenarios where public or individual welfare are increased, and scenarios where significant tangible and intangible costs arise. Consider a peer-to-peer scenario: Your phone (or in some years your glasses, and in a few more your contact lenses) will tell you the name of that person at the party whose name you always forget; or, it will tell the stalker in the bar the address where you live. Consider a third party firm scenario: The hotel will recognize and greet you as you enter the lobby with your luggage (because you friended them on a social network, or because - with or without your consent - the hotel enrolled in some identity recognition service sold by a social network); or, the salesperson will infer your credit score the moment you enter the dealership, and use a psychological profile (also calculated in real time from your online posts) to nudge you to accept a steep price for the car you wanted. Consider a government agency scenario: An investigative agency will be able to find missing or exploited children in databases of online photos; or, an administration will be able to identify from remote, high-definition cameras, all of the thousands of participants in a peaceful protest. More scenarios are unforeseeable today but will be commonplace tomorrow.

In short, face recognition could make our lives easier, or more comfortable, or more secure; conversely, it could limit our freedom, endanger our security, ease the extraction of consumer surplus, and chill free speech by creating a state of constant and ubiquitous surveillance.

Next, I will discuss the implications of face recognition for privacy as a final good: in this regard, there are reasons to believe that the process through which face recognition erodes our notion of privacy has not just started, but is well on its way. Note that the results of our experiments were limited by design: our self-imposed constraint consisted in only using publicly available data and technologies that other third parties and end-users could also get access to: off-the-shelf face recognition technology,[25] limited computational power accessed through cloud computing services, and limited amounts of facial images made publicly available by end users on online social networks. In reality, today, both governmental and private sector entities have access to more powerful computational tools and much larger (and more accurate) repositories of digital photos than we had.

Consider, for instance, Facebook – currently the largest social networking site. Many of its users (estimated at over 900 million worldwide,[26] with more than 90 billion of photos allegedly collectively uploaded[27]) choose photos of themselves as their "primary profile" image. These photos are often identifiable: Facebook has aggressively pursued a "real identity" policy, under which members are expected to join the network under their real names, under penalty of account cancelation.[28] Using tagging features and login security questions, the social network has successfully nudged users to associate their and their friends' names to uploaded photos. These photos are also publicly available: Primary profile photos *mus*t be shared with strangers under Facebook's own Privacy Policy. [29] Many members also allow those photos to be searchable from outside the network via search engines.

Online social networks such as Facebook are accumulating the largest known databases of facial images. Often, those images are tagged or attached to fully identified profiles, thus providing a linkage between a person's facial biometrics and their real names. Furthermore, many social network users post and tag *multiple* photos of themselves - and their friends, allowing biometric models of their faces, and those of other people as well, to become more accurate. Before Face.com was acquired by Facebook, for instance,[30] its mobile face recognition application Klik effectively used its own users as means of improving the recognition accuracy of its algorithms (since users were asked to select the correct name among a list of possible matches found by the application for a given face). This process would increase the future recognizability even of subjects who did not explicitly consent to more accurate biometric models of their faces being composed, or who had no knowledge of that happening.[31] Furthermore, such vast and centralize biometrics database can be at risk of third-party hacking.[32]

Online social networks are becoming today's de facto "Real IDs" – produced not by legislative mandate but technological capability. We must realize that the notions and expectations of privacy and anonymity, as we have known them for the history of human kind – the idea that, among strangers, you are a stranger, are facing a new challenge that we do not yet fully comprehend.

4. Implications

The evolution of face recognition technology is inescapable, but its applications will not all be equally desirable. Unfortunately, there is no obvious silver bullet that will allow society to continue to enjoy the benefit of face recognition divorced from its more concerning usages. There are, however, policy and technology mechanisms that are worth of investigation, and which carry trade-offs we are only beginning to appreciate: privacy enhancing technologies applied to face capture, detection, or recognition;[33] moratoriums on specific applications of face recognition;[34] explicit consent requirements to having one face's tracked, or matched, in public; do-not-recognize-me mechanisms; or privacy legislation that would place obligations on those who use facial recognition to collect the personal identity and thereby the personal information of others; and so forth. Unfortunately, the mere reliance on industry self-regulation is unlikely to find balance between uses and abuses of face recognition, due to the particular economic value of identified facial information, and recent history in the markets for personal data.

Identified facial information is especially valuable because facial biometric models are peculiarly sensitive and powerful instruments of identification and tracking. First, a person's face is a permanent identifier: it changes over time in patterns that computers are learning to predict, but it cannot be permanently altered to avoid detection without great cost.[35] Second, a person's face is a veritable conduit between her different persona: it can link a person's online world (for instance, her social network presence) to her offline world (the person walking in the street). Third, it can be captured remotely and surreptitiously, and therefore without individual consent or knowledge. Fourth, the technologies necessary to track and identify faces, as discussed, are becoming ubiquitous. As a result, control over vast repositories of identified facial information can give a firm unique power to serve and influence an array of other services and applications; competition for that control, therefore, will be fierce, at the likely cost of the privacy of end users.[36]

An analysis of recent history in the market for personal data also suggests that firms may engage in more invasive applications of face recognition over time. Currently, end-user applications of face

recognition have limited capabilities. Yet those limitations are less driven by technological constraints than by firms' concerns over consumers' reaction to too-aggressive deployment of face recognition. Evidence of this can be gleaned from firms' assurances that these services do not (yet) allow indiscriminate face recognition of everybody: for instance, Face.com developed the face recognition tagging services used by Facebook users --- but "if you choose to hide your Facebook tags, [Face.com] services will get blocked out when attempting to recognize you in photos."[37] However, if recent history of privacy in social networks is a guide, the current, almost coy applications of face recognition may be "bridgeheads" designed by firms to habituate end-users into progressively more powerful and intrusive services. Consider the frequency in which, in the past few years, a popular social network such as Facebook has engaged in practices that either a) unilaterally modified settings or defaults associated with users' privacy, so as to force increased sharing or disclosure;[38] and b) reflected a "two steps forward, one step backward" strategy, in which new services were enacted or proposed, then taken back or scaled down due to users' reaction to their invasiveness, and then enacted again, after some time had passed.[39] The fact that, as consumers, we do get eventually habituated to those new services does not necessarily prove that they come without risks: Our attention is captured by what we can see as their immediate benefits; what we pay less attention to are their privacy costs, as they are often delayed.[40]

In the absence of policy intervention, therefore, the patterns we are observing (increasing gathering and usage of individuals' facial biometrics data) are unlikely to abate. The risk exists that some firms may attempt to strategically use default settings, unilateral changes to interfaces and systems, and user habituation to nudge individuals into accepting more capturing and usage of facial data – creating a perception of *fait accompli* which, in turn, will influence individuals' expectations of privacy and anonymity.

Information is power. In the 21st century, the wealth of granular data accumulated about each individual, and the staggering progress of behavioral sciences in understanding how that knowledge can be used to nudge and influence individual behavior, make it so that control over personal information will imply power over the person. It does not matter whether this control will be exercised by a government or by a corporation: as control is tilting from data subjects to data holders, the very balance of power between different entities is at stake. Senators, I do not envy your position. We had the easy task – showing the problem. You have the much harder task of helping steer us towards its solution.

Thank you for inviting me to testify today. I look forward to answering your questions.

[1] See http://www.heinz.cmu.edu/~acquisti/

[2] A. Acquisti, 2010. “The Economics Of Personal Data and The Economics Of Privacy.” Commissioned By The OECD, For The OECD Roundtable On The Economics Of Privacy and Personal Data, Paris, December 2010. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf.

[3] A. Acquisti, 2004. “Privacy In Electronic Commerce and The Economics Of Immediate Gratification.” ACM Electronic Commerce Conference, 21-29.

[4] In this testimony, I use sometimes “face recognition” as a short-hand for machine-based, or computer, face recognition.

[5] R. Gross and A. Acquisti, 2005. “Information Revelation and Privacy in Online Social Networks." Proceedings of the 2005 Workshop on Privacy in the Electronic Society (WPES), ACM, 71-80, 2005; A. Acquisti and R. Gross, 2006. “Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.” Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science 4258, Springer, 36-58.

[6] A. Acquisti, R. Gross, and F. Stutzman, 2011. “Faces of Facebook: Privacy In The Age Of Augmented Reality.” Proceedings of Blackhat USA. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

[7] Some of the earliest works in this area include, e.g., W.W. Bledsoe, 1964. “The model method in facial recognition.” Tech. rep. PRI:15, Panoramic Research Inc., Palo Alto, CA; T. Kanada, 1973. “Computer recognition of human faces.” Birkhauser, Basel, Switzerland, and Stuttgart, Germany; M.D. Kelly, 1970. “Visual identification of people by computer.” Tech. rep. AI-130, Stanford AI Project, Stanford, CA.

[8] P.J. Phillips, 2011. “Improving Face Recognition Technology” Computer, 44(3), 84-86.

[9] For instance, computers outperform humans in recognizing unfamiliar faces: P.J. Phillips et al, 2007. “FRVT 2006 and ICE 2006 large-scale results.” National Institute of Standards and Technology, #7408.

[10] For instance, significant debate accompanied the usage of face recognition during Super Bowl 2001; see http://www.wired.com/politics/law/news/2001/02/41571.

[11] See http://picasa.google.com/support/bin/answer.py?answer=156272. More recently (in the summer of 2011) Google also acquired Pittsburgh-based face recognition company PittPatt.

[12] See http://support.apple.com/kb/ht344.

[13] See http://www.facebook.com/blog.php?post=403838582130. More recently (in the summer of 2012), Facebook has acquired Face.com.

[14] See http://www.face.com. The application is no longer available to end-users after Face.com was acquired by Facebook.

[15] See http://www.guardian.co.uk/media/pda/2010/sep/27/advertising-billboards-facial-recognition-japan.

[16] See http://www.scenetap.com.

[17] A. Acquisti, R. Gross, and F. Stutzman, 2011. “Faces of Facebook: Privacy In The Age Of Augmented Reality.” Proceedings of Blackhat USA. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

[18] See S. Garfinkel and B. Rosenberg, 2009. “Face Recognition: Clever or Just Plain Creepy?” MIT Technology Review, February 27.

[19] A. Acquisti and R. Gross, 2009. “Predicting Social Security Numbers From Public Data.” Proceedings Of The National Academy Of Science, 106(27), 10975-10980.

[20] P. Ohm, 2010. “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.” UCLA Law Review, 57, 1701.

[21] C. Jernigan and B.F.T. Mistree, 2009. “Gaydar: Facebook friendships expose sexual orientation.” First Monday,14(10).

[22] A. Acquisti and R. Gross, 2009. “Predicting Social Security Numbers From Public Data.” Proceedings Of The National Academy Of Science, 106(27), 10975-10980.

[23] P.J. Phillips, 2011. “Improving Face Recognition Technology” Computer, 44(3), 84-86.

[24] J. Farrell, 2011. “Can Privacy Be Just Another Good?” Remarks presented at University of Colorado at Boulder’s Conference on the Economics of Privacy.

[25] We used PittPatt, a face recognition application developed by former CMU researchers. Just a few days before our results were publicly presented, PittPatt was acquired by Google, thus the technology is no longer publicly available.

[26] See http://www.facebook.com/press/info.php?statistics.

[27] See http://www.quora.com/How-many-photos-are-uploaded-to-Facebook-each-day.

[28] See http://www.guardian.co.uk/world/2011/mar/09/chinese-blogger-mark-zuckerberg-dog.

[29] Consider: “Facebook is designed to make it easy for you to find and connect with others. For this reason, your name and profile picture do not have privacy settings,” from http://www.facebook.com/policy.php, accessed July 22, 2011.

[30] See http://news.cnet.com/8301-1023_3-57455287-93/facebook-acquires-face.com-for-undisclosed-sum/.

[31] At the time of writing, one’s images on Facebook by default can be tagged by people in their network, unless the individual explicitly opts-out. The power of default settings in nudging people’s privacy choices has been explored, among others, by A. Acquisti, L. John, and G. Loewenstein, 2010. “What Is Privacy Worth?” In Workshop On The Economics of Information Security. (Leading Paper, 2010 Future Of Privacy Forum's Best “Privacy Papers For Policy Makers” Competition.)

http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf. Furthermore, frequent users' errors in choosing privacy settings have been found by A. Acquisti and R. Gross, 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science 4258, Springer, 36-58.

[32] For instance, security researcher Ashkan Soltani exploited a vulnerability in Klik to gain access to non-public photos and other potentially private data of Facebook users. See F. Rashid, 2012. "Face.com Fixes Facebook Hijacking Flaw in KLIK Mobile App." SecurityWatch, PCMag.com, June 20, 2012.

[33] Research in this area has been carried out by, among others, Ralph Gross and Latanya Sweeney.

[34] See http://epic.org/2012/02/epic-calls-for-moratorium-on-f.html.

[35] Consider, for instance, plastic surgery. We are not referring to temporary solutions (such as masks and cosmetic make-up), whose costs increases with the amount of time the person has to carry them in the course of their lives.

[36] While studies have shown that a significant portion of consumers are willing to pay price premia to purchase from more privacy protective merchants (J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, 2011. "The Effect Of Online Privacy Information On Purchasing Behavior: An Experimental Study." Information Systems Research, 22, 254-268), it is not obvious that competition alone stimulates a market for privacy products. See, for more details. A. Acquisti, 2010. "The Economics Of Personal Data and The Economics Of Privacy." Commissioned By The OECD, For The OECD Roundtable On The Economics Of Privacy and Personal Data, Paris, December 2010.

[37] Extracted from Face.com FAQ in July 2011.

[38] Consider examples such as Facebook News Feed in 2006; Tagging in 2009; the changes in privacy settings in late 2009/early 2010; the lifting of cache time limits in 2010 (previously, user data accessed through APIs could only be cached by developers for 24 hours); the introduction of Facebook Places in 2010 (which allows others to tag a user in a certain location); the compulsory switch to "Timeline" in late 2011/early 2012; and the more recent switching of users to Facebook emails. These examples are discussed in work in progress by Alessandro Acquisti, Fred Stutzman, and Ralph Gross, and have been analyzed by research assistants at Carnegie Mellon University Seth Monteith and Nikolas Smart.

[39] Examples (also discussed in the work in progress mentioned in the previous footnote), include Beacon/Connect (2007-2008); and ToS change relative to the closing of a Facebook account in 2009.

[40] A. Acquisti, 2004. "Privacy In Electronic Commerce and The Economics Of Immediate Gratification." ACM Electronic Commerce Conference, 21-29.